Proceedings of the 4th NATIONAL CONFERENCE on Research and Development in Science,Engineering and Technology

NCRDSET 18

23.03.2018

Organized by

ST. ANNE'S
COLLEGE OF ENGINEERING AND TECHNOLOGY

Sponsored by

Indian Society of Technical Education

VOLUME - II

Proceedings of

ISTE sponsored

4th National Conference on Research and Development in Science, Engineering and Technology

NCRDSET ‘18

(Volume II)

23rd March 2018

Organised by

St. Anne’s College of Engineering and Technology

Anguchettypalayam, Panruti – 607106.

PREFACE

We are glad to present the proceedings of the Fourth National Conference on Research and Development in Science, Engineering and Technology (NCRDSET ‘18). The major goal and feature of the conference is to bring academic scientists, engineers, industry researchers together to exchange and share their experiences and research results, and discuss the practical challenges encountered and the solutions adopted.

This proceeding contains around 200 papers which has been spitted into two volumes one for Mechanical, Civil, Applied Sciences, Humanities and Electrical Engineering papers and other contains papers in the field Electronics, communications and Computer Science.

The theme of this conference was the key issues associated with science and technology in this rapidly evolving field of research and to promote contact between basic researcher and technological needs for real advanced materials and industrial applications.

We want to express our gratitude to all the members of conference committee, and reviewers who spared their valuable time, for their advice which have certainly helped to improve the quality, accuracy, relevance and the sincere efforts to maintain the quality of each paper selected for conference program and volume for publication. Also, we would like to thank every author and participant who has contributed to the success of the conference, and we truly hope to see you again in the next year of NCRDSET 2018.

We wish all attendees of NCRDSET 2018 an enjoyable scientific gathering.

M. SENTHAMARAI SELVI

23rd March 2018 **Convenor - NCRDSET’18**

ORGANISING COMMITTEE

CHIEF PATRON

Rev. Sr. Victoria, S.A.T
Secretary
St. Anne's College of Engineering and Technology

PATRON

Dr. R. Arokiadass, M.E., Ph.D.,
Principal
St. Anne's College of Engineering and Technology

CO - PATRON

Sr. Gnana Jency Salate Mary, S.A.T
Vice Principal
St. Anne's College of Engineering and Technology

CONVENOR

Mrs. M. Senthamarai Selvi,
Associate Professor & Head
Department of Computer Science and Engineering

CO - CONVENORS

Mr. D. Ommurugadasan,
Professor & Head
Department of Mechanical Engineering

Sr. Anita,
Associate Professor & Head
Department of Electronics and Communication Engineering

Mrs. S. Lese,
Associate Professor & Head
Department of Electrical and Electronics Engineering

Dr. A. John Peter,
Professor & Head
Department of Science and Humanities

DEPARTMENT OF ARCHITECTURE

NATIONAL INSTITUTE OF TECHNOLOGY

TIRUCHIRAPPALLI 620 015 TAMILNADU INDIA

Telephone: (0431) 2503550, 2503558 **Mobile:** +91 9894018599 **e-mail:** ktm@nitt.edu

19th March 2018,
Tiruchirappalli.

Greetings!

It is my great honor to participate as Chief Guest in the 4th "National Conference on Research and Development in Science, Technology, and Engineering" NCRDSTE-2018. I am very much impressed by the commitment of the St. Anne's College of Engineering and Technology, Panruti, to promote academic excellence and R&D in the science, technology, and engineering. The R&D sector in India is all set to witness some robust growth in the coming years. It is clear that NCRDSTE-2018 is concerned to form researchers among the students and faculties who are not only truly competent in their areas of expertise but also committed to supporting the emergence of new innovations and developments. This conference provides the platform for bringing together academicians, researchers, and practitioners not only to discuss recent research developments in the emerging science, technology, and engineering and also afford to assess on needed to be taken for in future, for the development of the country.

My heartfelt congratulations to the college management, faculties and the students in their continuing efforts to promote research and development in all fields. I sincerely hope that the conference becomes a grand success.

With best wishes,

(Dr. K. Thirumaran)

MESSAGE FROM SECRETARY'S DESK

Warm and Happy greeting to all. I am immensely happy that our college St. Anne's College of Engineering and Technology is organizing the 4th National Conference on **Research and Development in Science, Engineering and Technology [NCRDSET '18]** on 23.03.2018 and is going to present a collection of various technical papers in the proceedings.

Engineering and Technology in Research and development is an integral part that helps to understand and provide a interaction among dynamic research scholars, faculty members and students to disseminate the awareness of the recent developments and latest trends in the field of Science, Engineering and Technology.

I also congratulate authors, speakers, committee members, reviewers, sponsors, advisers and other members for their efforts in organizing and participating in this conference and wish the conference all the success. The holistic and comprehensive education provided in the College will enlighten the students and enable them to become employment-ready.

The dedicated principal, convener, Head of the departments, staff members and disciplined students are the added features of our college. The students are trained in all aspects to become a successful engineers and good citizens.

I wish the conference a great success.

Sr. Victoria, S.A.T.

Secretary
St. Anne's College of Engineering and Technology

MESSAGE FROM PRINCIPAL'S DESK

It is indeed a matter of immense pleasure to announce that, St. Anne's College of Engineering and Technology, is going to organize the 4th National Conference on " Research and Development in Science, Engineering and Technology" (NCRDSET'18) on 23rd March 2018.

I am confident that the conference discussions and the publication of the conference proceeding will bring opportunities among the academicians, research scholars and students to present their innovative ideas, most up-to-date findings, and technical proficiency in the various fields of Research. On behalf of St. Anne's College of Engineering and Technology, I heartily welcome the Honorable Keynote Speaker, eminent academicians, and all the paper presenters to NCRDEST '18.

My heartfelt wishes to HODs, staff members and students of our College for their efforts in organizing this conference.

I wish the conference a grand success.

Dr.R. Arokiadass, M.E., Ph.D.,

Principal
St. Anne's College of Engineering and Technology

MESSAGE FROM VICE-PRINCIPAL

"Two things help success in life.
The way you manage when you have nothing,
The way you manage when you have everything."

It is a great pleasure for me that our college is conducting Forth National level conference on "Research and Development in Science, Engineering & Technology - NCRDSET'18". The purpose of this conference is to bring together the researchers, experts from industry, academia, and other interested organizations to exchange information and new ideas in developments in the field of Science, Engineering & Technology. "Engineers are the people who can create practical solutions to our 21st century challenges of sustainability, housing and an ageing population. And we need more of them." As said by James Dyson, we the society need more Engineers who have interest to invent towards social welfare. I hope this Conference would certainly help everyone to have the latest updates and to have a better understanding to contribute more towards the need of society. On behalf of the management, I congratulate the Convener and the organizing committee. I thank all the participants who have come from various colleges to explore their views.

May God bless you all.

Sr. Gnana Jency Salate Mary, S.A.T.

Vice Principal

St. Anne's College of Engineering and Technology

TABLE OF CONTENT

ELECTRONICS AND COMMUNICATION ENGINEERING

IR Based Anti Piracy Screening System

[1]Julit Xavio X, [2]Mary D, [3]Punitha P,
[1, 2,3] Department of Electronics and Communication Engineering, St.Anne's College of Engineering and Technology Anguchettypalayam, Panruti
\

[4]Venkatesan V, AP, [5]RadhaKrishnan R, AP
mailto:rocky.radha@gmail.com, Mobile: 9750786839
[4,5] Department of Electronics and Communication Engineering, St.Anne's College of Engineering and Technology Anguchettypalayam, Panruti
\

Abstract– Cinema is a major entertainment for people in today's life. To entertain people a lot of investment is put on cinemas by the film – makers. Their effort is being ruined by few people by pirating the cinema content. They do it by capturing the video in mobile camera and upload it to websites or sell it to people and this goes on. There have been repeated attempts and pleas to kill piracy and save the film industry, members of film would have even staged protests and submitted memorandums to the government. In this paper, a technical method to prevent video recording in movie theatres is presented. An invisible light is projected from the screen to the whole audience that falls on the cameras which are optically sensitive to infra-red light inturn disturbing the acquisition functions of any camera making an illegal recording in the theatre useless.

Keywords: Anti-piracy, camcorders, fingerprint scanner, IR rays, screen.

I. INTRODUCTION

In today's age the growth of the Internet has led to many new innovations in the way it is used. Internet can provide fast access to any kind of information and media, and also the copyrighted contents."Piracy refers to the unauthorized duplication of copyrighted content that is then sold at substantially lower prices in the 'grey' market".Final copy of the movie content might get leaked before its release by the multiple teams working on them.The more common method is to film the movie inside a theatre and then uploading it on Websites or convert them to DVDs and sell them on the streets. Most box office releases are available online within a few days or even hours of the box office release.

Copyright law protects the value of creative work. Making unauthorized copies may subject one to civil and criminal liability.Night vision goggles are provided to movie hall staffs which would help them to notice any audience trying to record a movie while screening. Instead of treating every movie goer as a potential pirate, an anti-piracy screening system can be implemented inorder to make the pirate copy useless as well as having no effect on the audience.

II.EXISTING METHOD

It describes two level of authentication, card based and micro-controller keypad based. Two levels of authentication is useful for providing high security to the system but it is not compulsayr to give two different types of authentication.Since the authentication is used only to illuminate the IR LEDs. In this technique we are using one type of authentication to illuminate the array of IR LED. Therefore, only the authorized person can be able to ON or OFF of the LED. The authentication is provided by the Fingerprint scanner ie) GT511C3.

III. PROPOSED SYSTEM

This paper describes a system where in IR signals are transmitted towards movie audiences in the theaters which will wash out any silicon-CCD (charge coupled devices)-based digital camcorders, which makes the recorded video content unfit for illegal marketing. The proposed system contains a fingerprint scanner which is used to switch ON or OFF
Of the arrays of the IR LED. Since the IR rays are invisible to the human eyes but it is visible to electronic components.

IV.BLOCK DIAGRAM

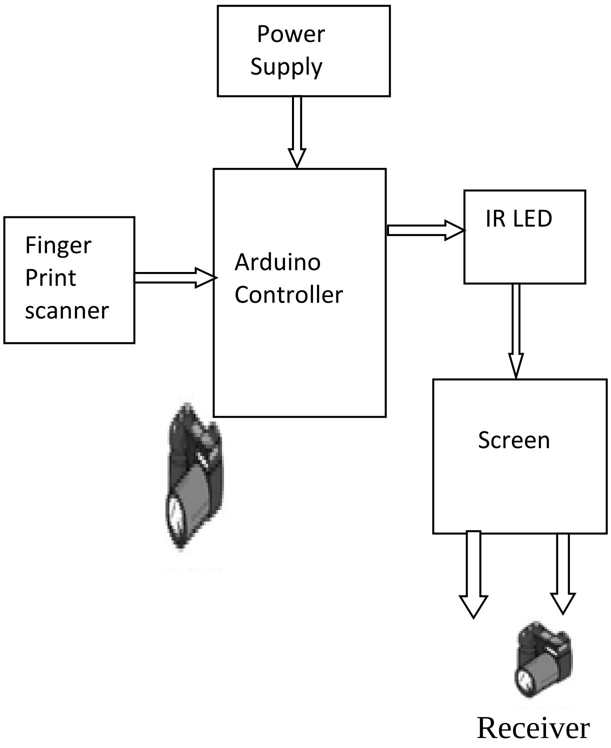


Fig.1Block diagram of the proposed system

V. DESCRIPTION

The components mentioned in the Block Diagram (Fig 1) are explained below:

Fingerprint scanner:

Fingerprints have been widely used as a mean of personal identification over a century.GT-511C3 FPS (fingerprint scanner) is a small embedded module that consist of an optical sensor mounted on a small circuit board. The fingerprint scanner automatically processes the scanned fingerprint.

The fingerprint scanner can store different fingerprints and the database of prints can even be downloaded from the unit and distributed to other modules. As well as the fingerprint "template", the analysed version of the print, you can also retrieve the image of the fingerprint and even pull raw images from the optical sensor.

Arduino:

Arduino is an open-source computer hardware and software company, project, and user community that designs and interactive objects that can sense and control objects in the physical world. It use a variety of microprocessors and controllers. The boards are equipped with sets of digital and analog input/output (I/O) pins that may be interfaced to various expansion boards (shields) and other circuits. The boards feature serial communication interfaces, including Universal Serial Bus (USB) on some models, which are also used for loading programs from personal computers. The microcontrollers are typically programmed using a dialect of features from the programming languages C and C++.

IRtransmitter:

IR Transmitter is used to control any device wireless, means remotely. The IR LED & photo transistor both of them have their sensitive area on their tip and their anode lead is longer than the cathode. The IR LED works between 1.6V-3.3V. IR wavelength ranges between 750nm-2500nm. Different IR LEDs may produce infrared light of differing wavelengths, just like different LEDs produce light of different colors. IR LEDs are usually made of gallium arsenide or aluminum gallium arsenide. In complement with IR receivers, these are commonly used as sensors. The appearance of IR LED is same as a common LED. Since the human eye cannot see the infrared radiations, it is not possible for a person to identify if an IR LED is working. A camera on a cell phone camera solves this problem.

Screen:

A projection screen is an installation consisting of a surface and a support structure used for displaying a projected image for the view of an audience. Projection screens may be permanently installed, as in a movie theater; painted on the wall; or portable with tripod or floor rising models. As in a conference room or other non-dedicated viewing space. Uniformly white or grey screens are used almost exclusively as to avoid any discoloration to the image, while the most desired brightness of the screen depends on a number of variables, such as the ambient light level and the luminous power of the image source.

VI. IMPLEMENTATION

This system employs a level of authentication. The Fingerprint scanner that is possessed by the respective theatre officer. It consists of information which is checked with preloaded fingerprint reference information stored in the fingerprint scanner. The output of the fingerprint scanner is passed on to the IR LED where it provides an illumination of the IR rays towards the audience through the screen.

On switching on the Arduino, fingerprint scanner gets activated for the fingerprints to be entered. If the fingerprints is verified then the output is given to the IR LED which is placed behind the screen. Therefore the output from the fingerprint scanner is used to control the IR LED.

The signals that are transmitted by IR LEDs placed behind and also along the perimeter of the screen are emitted towards the audience. So this invisible light disturbs the acquisition functions of the camera.

VII. EXPERIMENTAL RESULTS

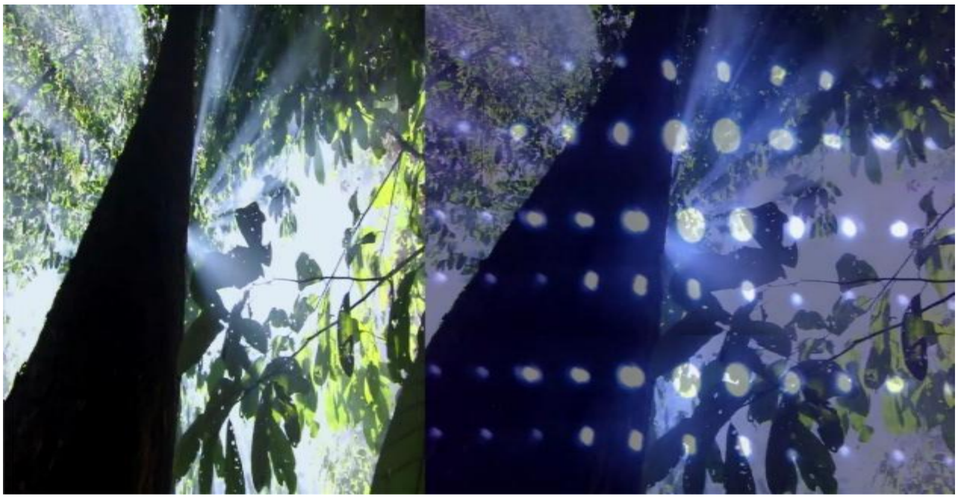


Fig 2(a) Normal picture (b) Picture after placing IRs behind and around the screen

On placing IR LEDs behind and around the screen in the cinema theatre, the video playing on the screen becomes blur or scrambled. Fig 2(b) will appear as Fig 2(a) for audience watching the movie because wavelength of IR (700nm-1mm) signal is longer than the visible light wavelength (400nm-700nm). Therefore, the audience will be able to watch the movie without any disturbance but since the camcorders are sensitive to IR light the recorded content becomes blur or unfit to watch.

VIII.CONCLUSION:

- This system provides a method to prevent the illegal recording of movies in theatres. Thus targeting the grey market of piracy.
- The IR transmitters are used in order to make the captured video useless.
- There can be various other application of this system which requires highdegree of privacy and security such as highly confidential conferences, meetings, research centres etc.,

IX.REFERENCES

[1] DLP based Anti Piracy Display System",ZhongpaiGao, GuangZhai, Xinolin Con, XiongKuo Min, 2014, IEEE

[2] "Card Based Anti piracy screening system"Akshatha, Deepika Vishwanath, 2016, ITSI-TEEE

[3] „MCT2 and MCT2E Optocouplers" Texas Instruments" revised October 1995

*[4] „Annoyance maximation for digital cinema anti piracy applications", M C larabi, V Rosselli,
2009, IEEE*

[5] „Remote Controls – Radio Frequency orInfrared", MartinGotschlich,Infineon Technologies AG, 2010

[6] „Evaluation Test performed over a proposed anti piracy system for Digital vector Data sets",Colonel A Bacci, Director, Dr C Lopez, 2003 Cambridge Conference

Implementation of an efficient Energy Detection Technique for Spectrum Sensing in Cognitive Radio

Mrs. M. Vaidehi
Professor,
Department of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Ms. S. Devika
Assistant Professor,
Department of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Mrs. C. Suganya
Assistant Professor,
Department of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Abstract-The radio frequency spectrum is a scarce natural resource and its efficient use is of the utmost importance. The spectrum bands are usually licensed to certain services, such as mobile fixed broadcast, and satellite, to avoid harmful interference between different networks. Most spectrum bands are allocated to certain services but worldwide spectrum occupancy measurements show that only portions of the spectrum band are fully used. Moreover, there are large temporal and spatial variations in the spectrum occupancy. In the development of future wireless system the spectrum utilization functionalities will play a key role due to the scarcity of unallocated spectrum. Moreover, the trend in wireless communication system is going from fully centralized system into the direction of self-organizing system where individual nodes can instantaneously establish ad hoc networks whose structure can change over time. Cognitive radio, with the capabilities to sense the operating environment, learn and adapt in real time according to environment creating a form of mesh network, are seen as a promising technology.

The paper presents an overview of cognitive radio; various spectrums sensing technique used in CR and also describe the state-of-the-art techniques in cognitive radio standards and regulation. In this project we have implemented and analyzed a energy detection technique for spectrum sensing in CR.

Keywords: Cognitive Radio, Spectrum Sensing, Energy Detection, Primary user, Secondary user, Threshold, Probability of detection, Probability of false alarm.

I. INTRODUCTION

With the development of a host of new and ever expanding wireless applications and services, spectrum resources are facing huge demands. Currently, spectrum allotment is done by providing each new service with its own fixed frequency block. As day passes demand for spectrum are expected to increasing rapidly and it would get in future. As more and more technologies are moving towards fully wireless system, demand for spectrum is enhancing.

Most of the primary spectrum is already assigned, so it becomes very difficult to find spectrum for either new services or expanding existing services. At Present government policies do not allow the access of licensed spectrum by unlicensed users, consists them instead to use several heavily populated, interference-prone frequency bands. As the result there is huge spectrum scarcity problem in certain bands.

In particular, if the radio spectrum is scanned, including the revenue-rich urban areas, it can be seen that some frequency bands in the spectrum are unoccupied for some of the time and many frequency band are only partially occupied, whereas the remaining frequency bands are heavily used.

The radio spectrum is limited resource and is regulated by government agencies such as telecom Regulation Authority of India (TRAI) in India, Federal Communication Commission (FCC) in the United States.

Cognitive radio is a novel technology which improves the spectrum utilization by allowing secondary user to borrow unused radio spectrum from primary licensed users or to share the spectrum with the primary users. As an intelligent wireless communication system, cognitive radio is aware of the radio frequency environment, selects the communication parameters (such as carrier frequency, modulation type, bandwidth and transmission power) to optimize the spectrum usage and adapts is transmission and reception accordingly.

By sensing and adapting to the environment, a cognitive radio is able to fill in the spectrum holes and serve its user without causing harmful interference to the licensed user. To do so, the cognitive radio must continuously sense the spectrum it is using in order to detect the re-appearance of the primary user.

2. DEFINITIONS

Simon Haykin defines Cognitive radio is an intelligent wireless communication system that is aware of its surrounding environment and uses the methodology of understanding by building to learn from the environment and adapt its internal states to statistical variations in the incoming radio frequency stimuli by making corresponding changes in certain operating parameters in real time, with two primary objectives in mind:

- highly reliable communications whenever and wherever needed
- efficient utilization of radio spectrum

"Radio whose control processes permit the radio to leverage situational knowledge and intelligent processing to autonomously adapt towards some goal."

2.1. Cognitive Cycle:

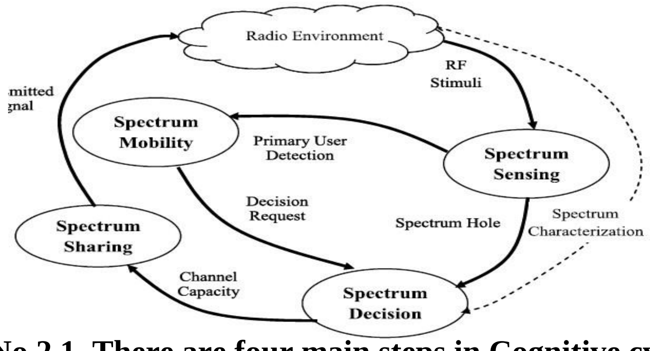


Figure No 2.1. There are four main steps in Cognitive cycle

1. **Spectrum Sensing**: It refers to detect the unused spectrum and sharing it without harmful interference with other users. It is an important requirement of the Cognitive Radio network to sense spectrum holes, detecting primary users is the most efficient way to detect spectrum holes.
2. **Spectrum Management:** It is the task of capturing the best available spectrum to meet user communication requirements.
3. **Spectrum Mobility:** It is defined as the process where the cognitive user exchanges its frequency of operation
4. **Spectrum Sharing**: This refers to providing a fair spectrum scheduling method among the users. Sharing is the major challenge in the open spectrum usage.

3. SPECTRUM SENSING

3.1 Introduction

An important requirement of the CR is to sense the spectrum holes. It is designed to be aware of and sensitive to the changes it's surrounding. The spectrum sensing function enables the cognitive radio to adapt to its environment by detecting the primary users that are receiving data within the communication range of a CR user. In reality, however, it is difficult for a cognitive radio to have a direct measurement of a channel between primary transmitters.

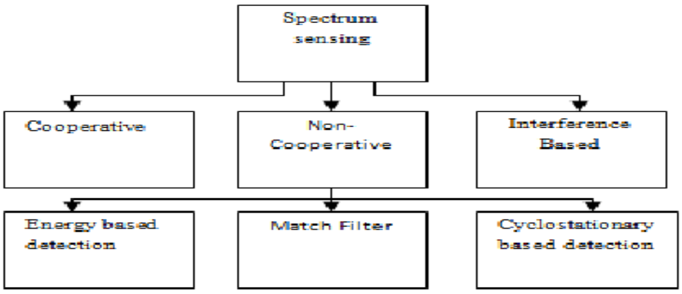


Figure No 3.1 Classification of Spectrum Sensing Techniques

3.2 Classification of Spectrum sensing techniques

- **Matched filter detection**
- **Energy detection**
- **Feature detection**
- **Cooperative detection**
- **Interference-based detection**

In this project we used energy detection technique.

3.3. Energy Detection

If the secondary user cannot gather sufficient information about the PU signal, the optimal detector is an energy detector, also called as a radiometer.

It is common method for detection of unknown signals. The block diagram of the energy detector is shown in Figure 4.2.

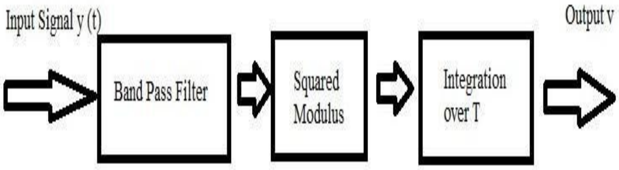


Figure No 3.2. Energy detection

First, the input signal y(t) is filtered with a band pass filter (BPF) in order to limit the noise and to select the bandwidth of interest. The noise in the output of the filter has a band- limited, flat spectral density. Next, in the figure there is the energy detector consisting of a squaring device and a finite time integrator.

The output signal V from the integrator is $\boldsymbol{V = 1/T \int_{t-T}^{t} |y(r)|^2 dr}$

Detection based on local observations of CR users. The spectrum can be classified into three types by estimating the incoming RF stimuli, thus, black spaces, grey spaces and white spaces. Black spaces are occupied by high power local interferer some of the time and unlicensed users should avoid those spaces at that time. Grey spaces are partially occupied by low power interferers but they are still candidates for secondary use. White spaces are free RF interferers except for ambient noise made up of natural and artificial forms of noise e.g. thermal noise, transient reflection and impulsive noise. White spaces are obvious candidates for secondary use.

The goal of the spectrum sensing is to decide between the two hypotheses, namely

$$\mathbf{x\ (t) = n(t)\ ,H0}$$

$$\mathbf{x\ (t) = hs\ (t) + n(t)\ ,H1}$$

Where X(t) is the signal received by the CR user, s(t) is the transmitted signal of the primary user , n(t) is the AWGN band h is the amplitude gain of the channel. H0 is a null hypothesis, which states that there is no licensed user signal. Generally, the spectrum sensing techniques can be classified as transmitter detection, cooperative detection, and interference-based detection, as shown in Fig 4.1.

Finally, this output signal V is compared to the threshold "n" in order to decide whether a signal is present or not. The threshold is set according to statistical properties of the output V when only noise is present. The probability of detection Pd and false alarm Pf are given as follows.

$$\boldsymbol{pd} = \{\boldsymbol{y} > \lambda\backslash H\mathbf{1}\}$$

$$\boldsymbol{pf} = \{\boldsymbol{y} > \lambda\backslash Ho\}$$

From the above functions, while a low Pd would result in missing the presence of the primary user with high probability which in turn increases the interference to the primary user, a high Pf would result in low spectrum utilization since false alarm increase the number of missed opportunities.

Since it is easy to implement, the recent work on detection of the primary user has generally adopted the energy detector. However, the performance of energy detector is susceptible to uncertainty in noise power. In order to solve this problem, a pilot tone from the primary transmitter is used to help improve the accuracy of the energy detector. The energy detector is prone to the false detection triggered by the unintended signals.

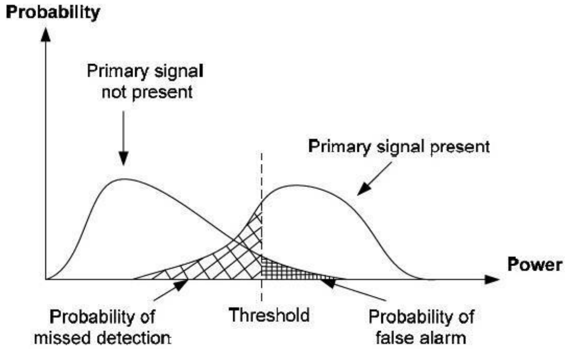

Probability
Primary signal not present
Primary signal present
Power
Probability of missed detection
Threshold
Probability of false alarm

Figure No 3.3.Trade-off between missed detection and false alarm

A simple energy detector works poorly for frequency hopping spread spectrum signals. The channelized radiometer is multichannel receiver that has several energy detectors that integrate energy in many frequency bands simultaneously. It is especially useful detecting frequency hopping spread signals. An analysis of the effects of frequency sweeping on a channelized radiometer is presented in. It is assumed that the signal to be detected uses slow frequency hopping and that sweeping is faster than hop dwell time.

In a practical signal detection system, the instantaneous bandwidth may be limited. In frequency sweeping, the centre frequency is changed as a function of time to cover a wider bandwidth. Numerical examples in demonstrate that if the number of hops observed per decision is small, sweeping can be necessary to get the desired performance. When the channel is fading, the best performance s obtained using fast sweeping. The drawback of channelized radiometer approach compared to a simple energy detector is the increased complexity.

4. SIMULATION DIAGRAM OF COGNITIVE RADIO USING ENERGY DETECTION TECHNIQUE

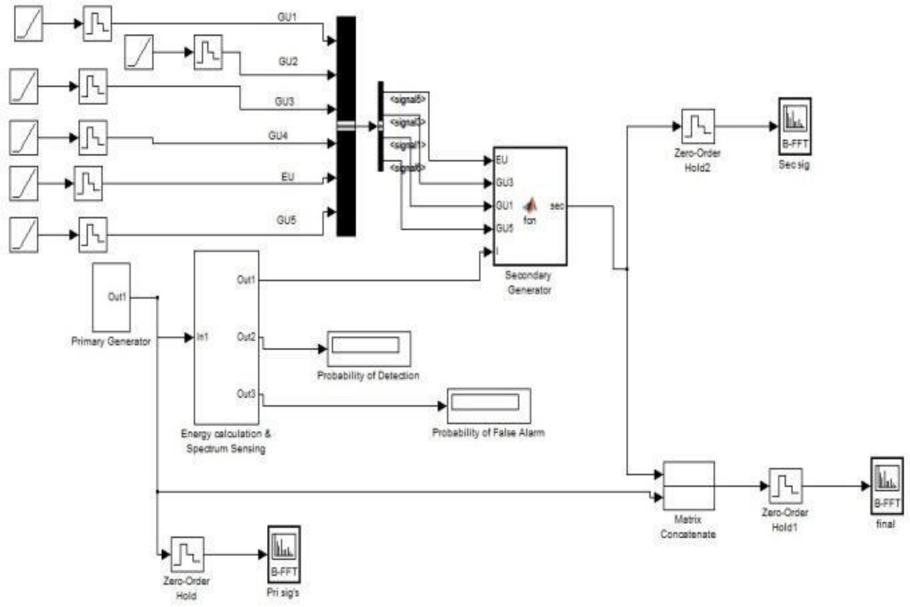


Figure No 4.1. Implementation block for energy detection

4.1.Primary Generator Block

The block representing the primary signal generation is shown in figure 4.2.

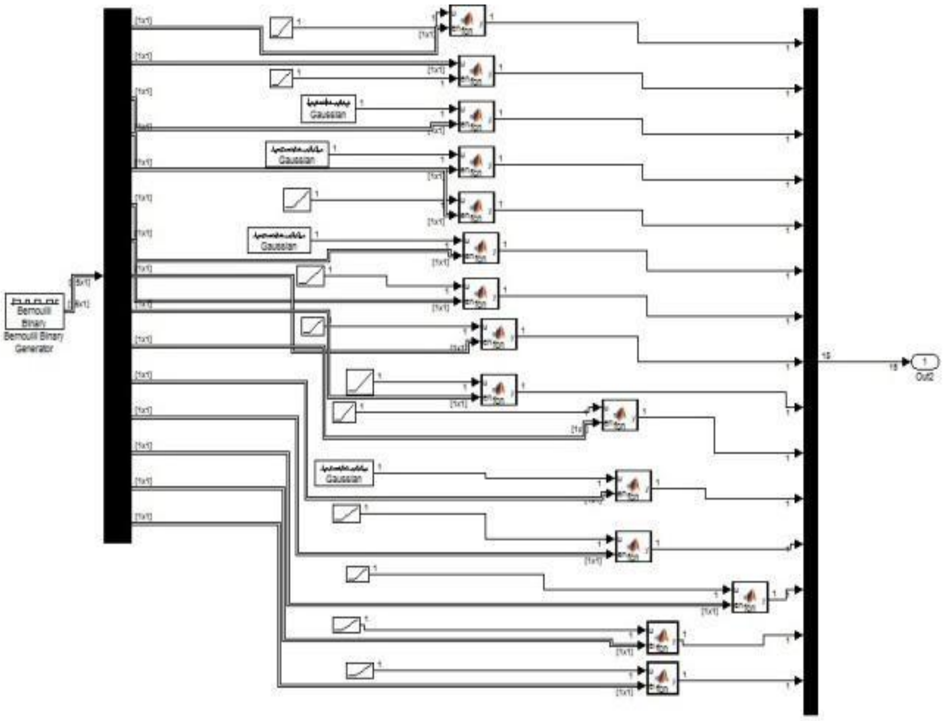


Figure No 4.1. Primary Generator block

4.2. Energy detection & Spectrum Sensing block

The block representing the Secondary signal generation is shown in figure 5.2.

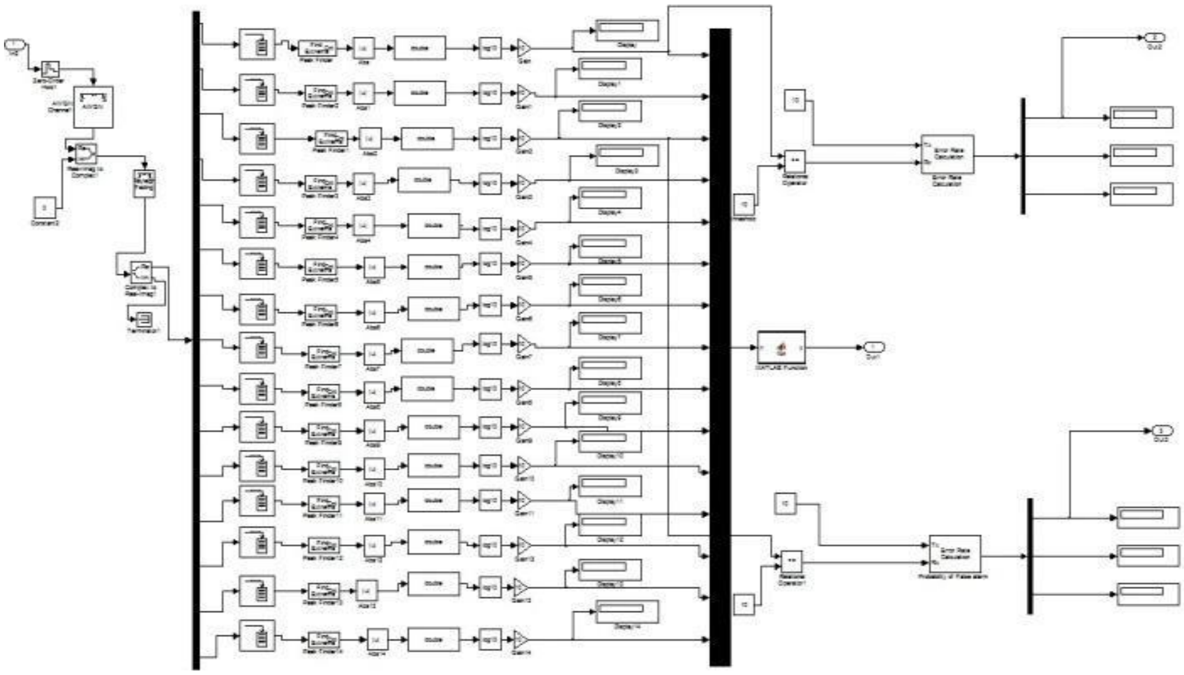


Figure No 4.2. Energy detection and spectrum sensing block

5. RESULTS & ANALYSIS

This chapter represents the plots obtained after analysis.

5.1. Scope Plots

The following figures represented the plots of "Primary signal scope", "Secondary signal scope" and "primary and secondary signal scope" of the simulated model, respectively.

In figure 5.1, the peaks represented the generated primary signal and the lines represent the noise in the vacant frequency slots.

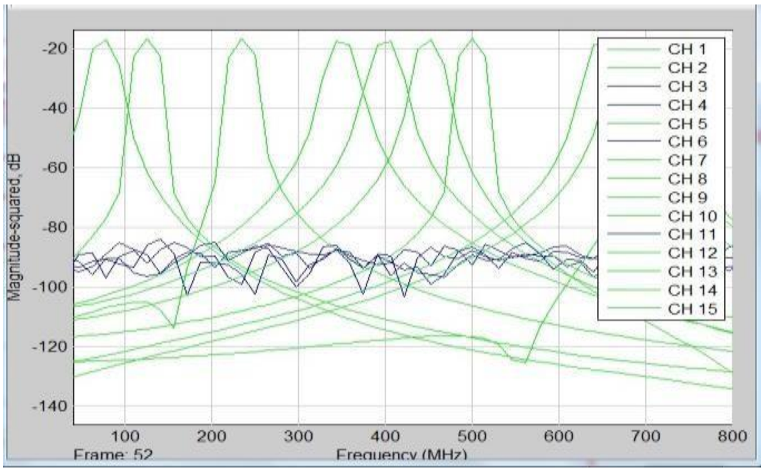


Figure No 5.1. Scope plot representing Primary signals

Figure 5.2, the secondary signal generated on the vacant frequency slots identified by energy detection, are shown.

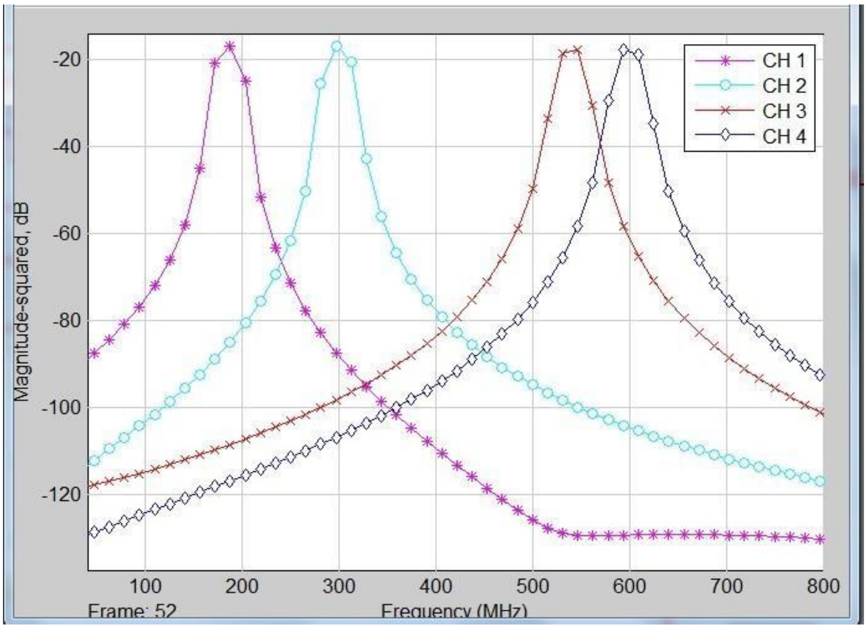


Figure No 5.2.Scope plot representing Secondary signals

In figure 5.3, all of the generated signals present in the spectrum band are represented with green peaks representing primary signals, color peaks representing secondary signals and black lines representing noise signals.

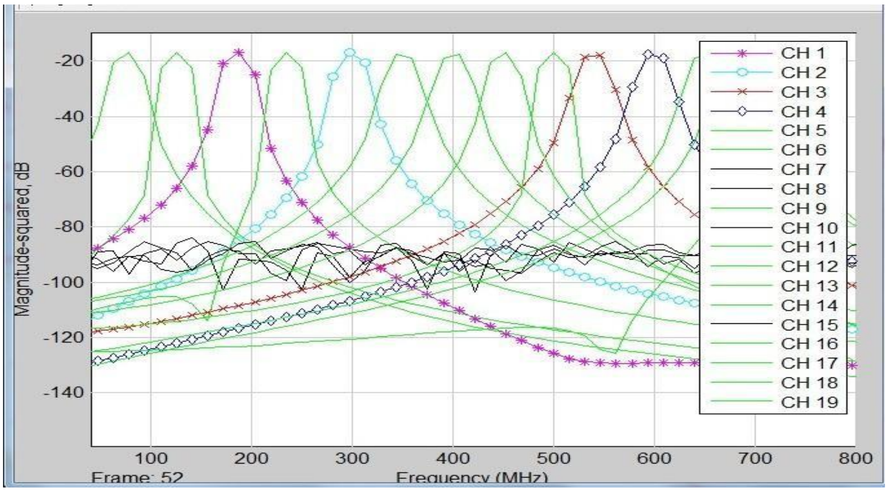


Figure No 5.3. Scope plot representing Primary & secondary signals

6. CONCLUSION

This work presented here has been implemented and analyzed successfully.

- It can be seen from figure 5.1 that primary signals have been generated successfully.
- It can be seen from figure 5.2 that energy calculation and detection of generated primary user signal have been done & empty slots have been found successfully.
- It can be seen from figure 5.3 that secondary user signals have been generated on allocated vacant slots with priority consideration.

REFERENCES

[1] Alexander M. Wyglinski, —*Cognitive Radio Communication and Networks*, Elsevier Publication

[2] Rozeha A. Rashid, Abdul Hadi Fikri Bin Abdul Hamid, Norsheila Fisal, Sharifah Kamilah SyedYusof, *"Efficient In-Band Spectrum Sensing"* in International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 6 (2016) pp 4563-4568 © Research India Publications. http://www.ripublication.com 4568 Swarm Intelligence for Cognitive Radio Network". Canadian journal of electrical and computer engineering, vol. 38, no. 2, spring 2015.

[3] Joanna Wallace et al.,—*Cognitive Radio Technology: System Evolution*‖, IEEE, 4th Edition of International Conference on Wireless Networks and Embedded Systems ,2015

[4] Gianmarco Baldini et al., —*The Evolution of Cognitive Radio Technology in Europe : Regulatory and Standardization Aspects* ,Elsevier, Telecommunications Policy 37 (2013) 96–107

[5] Ila Sharma, "*A Novel Approach for Spectrum Access Using Fuzzy Logic in Cognitive Radio*," Department of Electronics and Communication Engineering Jaypee University of Information Technology, Waknaghat, Solan-173 234, India I.J. Information Technology and Computer Science, 2012, 8, 1-9 Published Online July 2012 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijitcs.2012.08.01.

[6] Management, Bilaspur, Gurgaon, India. International Journal of Advances in Engineering & Technology, July 2011

[7] Mithun Chakraborty R.Bera, P.Pradhan, S.Sunar "*Spectrum sensing and Spectrum shifting implementation in a Cognitive Radio based IEEE 802.22 Wireless Regional Area Network, "* (IJCSE) International Journal on Computer Science and Engineering Vol.2, No. 04,2010, 1477-1481.

Analog Low Noise Amplifier Circuit Design and Optimization

Mr. V. Venkatesan[1], Mr.S.Durai Raj[2]
[1, 2] Assistant Professor,
Department of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Abstract* - With the increasing use of wireless communications, there emerges a trend towards integrating multiple wireless functionalities into one mobile device. Recently we have been observing a paradigm shift in the integrated wireless transceiver design where several narrow-band receivers customized for dedicated applications, e.g. cellular, wireless LAN (Local Area Network), and PAN (Personal Area Network) are replaced by one single circuit which support different standards operating on different frequency band is called —Universal Receiver. To support multiple standards which have different modulation techniques put tough performance requirement for noise, gain and matching of universal receiver design. Realizing Analog to digital converter for universal receiver for the RF signal without Low Noise Amplifier (LNA) is practically very difficult using current technology. The LNA and mixer are relaxing the stringent performance requirements of the analog to digital converter. In LNA design has performance trade-off among noise, gain, linearity, matching and power consumption. In the research designed and proposed two narrowband LNAs and three wideband LNAs for the Bluetooth, GPS, UWB and 4G technologies. Detailed analysis of all LNAs is carried out. All the LNAs design using 0.18µm RFCMOS model and simulate the design using Advanced Design System RF circuit simulator software.

***IndexTerms*—DE and PSOAlgorithms.**

I. INTRODUCTION

Motivation the demand of wireless transceiver RFICs is exp expanding rapidly because of its huge market ranging from pagers, cordless phones, cell phones, WLAN terminals, nodes for sensor networks and GPS to recently introduced DAB/DVB enabled PDAs [1]. These diverse range of mobile terminals have their own standard and require separate RF front-end and digital resources for baseband processing. As per today's demand modern mobile terminals should support WLAN, Bluetooth, ZigBee, GSM, 3G, GPS, LTE, IEEE 802.11a/b/g and WiMax etc. wireless communication standards. This demands the mobile terminals to be flexible in nature with low power and low cost..

Therefore, the designer is urged to integrate all radio blocks on a single chip along with hardware reuse/sharing which not only results in cost reduction due to reduced silicon area but allows exclusion of separate RF packaged chips at the same time. On-chip integration and placing a lower limit on the power consumption of performance centric analog circuits helps to reduce the power consumption. This mobile terminal is termed as Universal receiver.

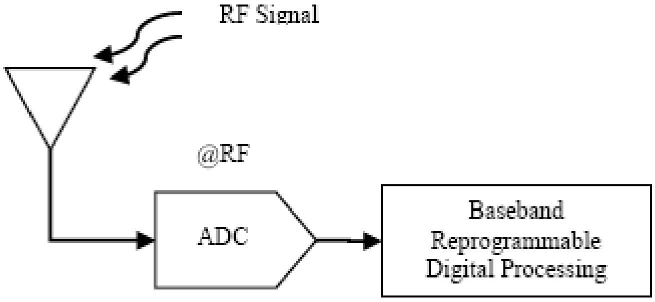


Fig1: Ideal universal radio architecture

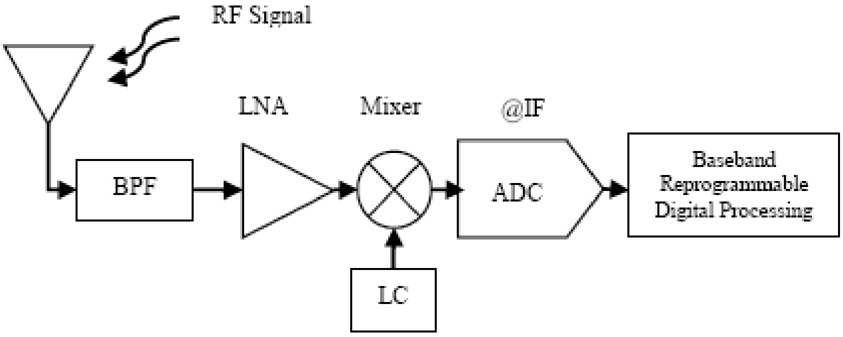


Fig2: Practical universal radio architecture

Ideal universal receiver as shown in Fig. 1 is still not a reality because of design challenges in domains of antenna, RF Front-end, A/D & D/A conversion and baseband processing. It puts very tough requirements on the dynamic range, speed, noise performance and linearity of A/D converter. An LNA relaxes the noise performance and dynamic range requirements while the frequency translation block reduces the speed requirements of the A/D converter. That is why, all multistandard, multiband receiver designs reported to date incorporate some sort of low noise amplifier.

The design specifications of next generation wideband LNAs should have S11≤−10 dB, NF≤ 3.5 dB, IIP3≥-5 dBm, Flat gain across the entire bandwidth and unconditional stability over entire frequency range. These requirements must be fulfilled without any compromise on silicon area and power consumption compared to narrowband LNAs, making them suitable for portable and hand-held applications.

II.LNA IMPLEMENTATION APPROACHES

Multi band multi mode LNA to support multiple standards can be obtain using three possible ways: (i) using a narrowband LNAs for each standard which results in high power consumption as well as higher cost due to large Si area , (ii) using a reconfigurable/band switching/multiband LNA. This allows more compactness and power saving but still occupies large area because of tuning inductors (iii) using wideband LNA which allows simultaneous multiband operation with low cost and small area. Wideband LNA is good solution of accommodate multiple standards.

2.1 LOW NOISE AMPLIFIER (LNA) PERFORMANCE PARAMETERS

Major performance parameters of LNA are: a) Noise Figure (NF) b) Power Gain (S21) and Input matching (S11) c) Linearity (IIP3) d) Power consumption e) Stability.

a).Noise Performance

The fundamental noise performance parameter is the Noise Factor (F), which is defined as the ratio of the total output noise power to the output noise due to input source. If the Noise Factor is expressed in decibels it is called the Noise Figure (NF) NF = 10log(F)

$$\mathrm{SNR} = \frac{\mathrm{P_{signal}}}{\mathrm{P_{noise}}}$$

$$\mathrm{F} = \frac{\mathrm{P_{si}}/\mathrm{P_{ni}}}{\mathrm{P_{so}}/\mathrm{P_{no}}}$$

A low-noise amplifier (LNA) is first amplifier stage of a receiver. Overall noise of multistage amplifier receiver is

$$NF_{tot} = 1 + (NF_1 - 1) + \frac{NF_2 - 1}{A_{p1}} + \cdots + \frac{NF_m - 1}{A_{p1} \ldots A_{p(m-1)}}$$

It is also known as Friis formula which is named after the Danish-American electrical engineer Harald T. Friis. Total receiver noise figure is dominated by the first few stages, especially the very first stage (namely the LNA). This is the rationale behind why the first stage amplifier needs to have as small of noise figure as possible.

b).Power gain and input matching

Other design performance parameter is Power gain (S21) it should have as high as possible to increase weak signal received from antenna. Measure of power gain can be obtained by S parameter S21. It is very important that the input impedance of the LNA is matched to a certain value, most commonly 50 Ω. A measure of the quality of the input match can be obtained by S11. If we assign the input port of an LNA to be port 1, S11 will be a complex number representing the ratio of how much power is reflected from port 1 to how much power is applied to port 1. So the magnitude of S11 (normally expressed in dB) is desired to be as small as possible (S11 = -∞ for a perfect impedance match). And the reason that it should be matched to 50 Ω is that most antennas have characteristic impedance of 50 Ω.

c).Linearity

The linearity of the LNA is another concern that must be taken into account. Linear operation is crucial, particularly when the input signal is weak with a strong interfering signal in close proximity. This is because in such a scenario there is a possibility for undesired inter-modulation distortion such as blocking and cross modulation.

Third-order intercept (IP3) and 1-dB compression point (P1dB) are two measures of linearity.IP3 shows at what power level the third-order inter-modulation product is equal to the power of the first-order output. IIP3 and OIP3 are the input power and output power respectively, that corresponds to IP3. P1dB shows at what power level the output power drops 1dB, as a consequence of non-linearity, relative the theoretical linear power gain, By knowing either IP3 or P1dB the other can be estimated with the following rule-of-thumb formula: IIP3=p1dBm+10dBm.

d).Power consumption

Power consumption is another design specification that needs to be closely inspected. Considering only the noise performance and linearity can lead to biasing solution that makes the power consumption simply too big to be practically realized. Increased incorporation of RF systems into hand-held device makes it necessary to minimize power consumption in order to maximize battery life.

e).Stability

In the presence of feedback paths from the output to the input, the circuit might become unstable for certain combinations of source and load impedances. An LNA design that is normally stable might oscillate at the extremes of the manufacturing or voltage variations, and perhaps at unexpectedly high or low frequencies. The stability factor is given

$$K = \frac{1+|\Delta|^2 - |S_{11}|^2 - |S_{22}|^2}{2|S_{21}||S_{12}|}$$

as in

Where, When K > 1 and < 1, the circuit is unconditionally stable.

As we can see, the design of an LNA is a multi-dimensional optimization problem. There are lots of trade-offs involved because the optimization of each individual specification does not arrive at the same sizing or biasing solution. This requires that the designer consider what is the best combination of performance specifications for the intended application of the LNA.

III Filter LNA topology

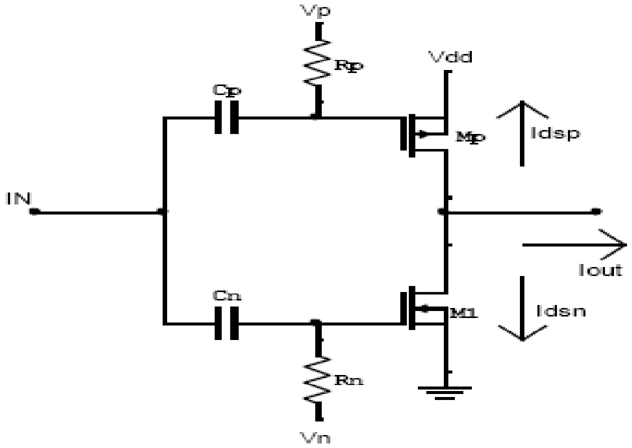
The band pass filter is used which resonant at entire band to provide wideband matching. Filter LNA has good performance while dissipating low power. Various types of filters are used like three-section band pass Chebyshev filter , LC filter, dual RLC filter, Miller effect input matching filter , high pass filter ,a π-matching LC filter and transformer based input matching network of such LNAs.

This topology is implemented with CS inductive degeneration stage to achieve good NF, Low power consumption, high gain and wideband input matching. Due to larger value of inductors in filter require off chip components.

The LNA presented in (3–5 GHz, 0.18μm CMOS) used only one inductor at the gate addition to a source degeneration inductor. Here exploitation of Miller effect is providing wideband matching. This approach reduce NF (≤2.3 dB) and chip area with the cost of poor linearity (P1dB =−23 dBm). The LNA (0.18μm CMOS) [24] provides wideband operation (3.1–10.6 GHz) with low power consumption (9.4 mW) by using current reuse at a cost poor linearity (IIP3 of−13 dBm).

4. Highly Linear noise cancelling wideband LNA design and optimization

We have design another highly liner partial noise cancelling wideband LNA for support Bluetooth, WiMax, IEEE 802.11a/b/g, LTE, 3GPP applications.



Complementary push pull LNA with resistive feedback

7.3.1 Circuit design

Figure shows the CMOS Inverter configuration amplifier. It consists of two transistors NMOS and PMOS. The signal is input from the tied gate of NMOS and PMOS and the output is taken from drain of both transistor. The drain current of both transistors can be expressed as follows:

$$i_{dsn} = g_{1A}V_{gs} + g_{2A}V_{gs}^2 + g_{3A}V_{gs}^3 + \cdots$$

$$i_{dsp} = -g_{1B}V_{gs} + g_{2B}V_{gs}^2 - g_{3B}V_{gs}^3 + \cdots$$

$$i_{out} = i_{dsn} - i_{dsp} = (g_{1A} + g_{1B})V_{gs} + (g_{2A} - g_{2B})V_{gs}^2 + (g_{3A} + g_{3B})V_{gs}^3$$

Where g1, g2 and g3 are the main transconductance, second-order and third-order nonlinearity coefficients respectively. The second order nonlinearity is cancel in output due out off phase signal by NMOS and PMOS. The optimum biasing is used to obtain a high IIP3 by reducing the total g3, the IIP3 can be calculate as follows:

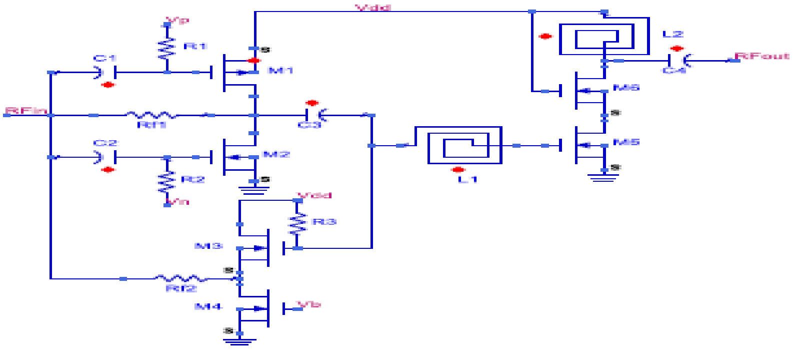
$$A_{IIP3} = \sqrt{\frac{4}{3}\left|\frac{g_1}{g_3}\right|}$$

With a simple analysis, this configuration employs two PMOS and NMOS gain devices to boost the overall transconductance, leading to high gm. With the proposed technique, reducing g3 and increasing g1 leads to highly linear and high gain performance over a wide range of frequencies.

a)Noise analysis

In CMOS inverter the value of the feedback resistance plays an important role in deciding the amount of noise added to the input. There is tread off between noise figure and wideband input matching: higher value of feedback resistor decrease NF but it not provides wider band input matching and vice versa. . This tread off can be avoid by using common drain (CD) active feedback. Trough CD feedback we can add one more degree of freedom to set NF and input matching for wideband. Using CD feedback cancel some amount of noise by adding out off phase noise signals

Design schematic



Circuit Description:

The first stage of proposed Wideband LNA consist shunt restive and common drain active feedback provide wideband matching and partial cancel noise to improve NF. In common source amplifier has a tradeoff between noise performance and tranconductance of amplifier. By using common drain active feedback we can set independent transconductance and noise performance. The second stage is a cascade amplifier for high gain with series and shunt inductive peaking to achieve a wider bandwidth. Value of inductor L2 and capacitor C2 set such that it resonance at middle of interested band. Drain inductor L3 is extending the bandwidth and improve the gain at high frequencies.

Conclusion

From the results Highly Linear noise cancelling wideband LNA design shows that our design provide flat more power gain in interested band compare to work published in literature. Our next highly linear wideband LNA design provide good linearity. To support ultra wideband applications require 3.1 to 10.6 GHz wideband high power gain LNA. Our ultra wideband high power gain LNA provide 20-34 dB gain which is highest compare to work published in literature and it support low transmit power ultra wideband applications.

REFERENCES

[1] Abidi, —The path to the software-defined radio receiver, IEEE J. Solid State Circuits 42 (5) (2007).

[2] J. Mitiola,The software radio architecture, IEEE Commun. Mag. 33 (5) (1995) 26–38

[3] T. H. Lee, The Design of CMOS Radio-Frequency Integrated Circuits, 2nded., Cambridge University Press, Cambridge, U. K, 1998.

[4] C. Toumazou, G. S. Moschytz, B. Gilbert, Trade-offs in Analog Circuit Design: The Designer's Companion,Part1,Springer,2004.

[5] H. Hashemi, A. Hajimiri, —Concurrent multiband low-noise amplifiers theory,design and applications, IEEE Trans. Microwave Theory Tech. 50(1) (2002)288–301.

[6] G. Sapone, G. Palmisano, —A 3–10GHz low-power CMOS low-noise amplifier for ultra-wideband communication, IEEE Trans. Microwave Theory Tech. 59 (3) (2011).

[7] R. Roovers, D. M. W. Leenaerts, J. Bergervoet, K. S. Harish, R. C. H. Beek, G. Weide, etal., —An interference robust receiver for ultra-wideband radio in SiGe BiCMOS technology, IEEE J. Solid-State Circuits 40 (12) (2005) 2563–2572.

Movable Pick & Place Robotic Arm

N. Gokula Krishnan[1], G.Ramachandran[2], S.Vignesh[3],

[1,2,3] Department of Electronics and Communication Engineering
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106

Ms. S.K. Suriya A P[4], Ms. S. Devika A P[5]

[4,5] Assistant Professor, Department of Electronics and Communication Engineering
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106

suriyakuberamoorthy@gmail.com, Mobile: 9578573293

Abstract — A robotic arm is designed using arduino to pick and place the objects via user commands. It will pick and place an object from source to destination safely. The robot is controlled using android based smart phones through Wi-Fi. Based on the commands given by the user the robot moves accordingly. At the receiver end there are five motors interfaced with the Arduino. Two for the vehicle movement and the remaining three are for arm and gripper movement.

Keywords — *Pick and place robotic arm, Remote XY app, Wi-Fi module.*

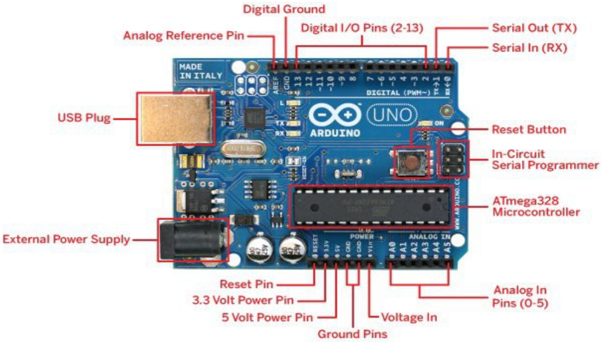
I. Introduction

Robotics gained more importance in the modern era since it require less cost to operate than a human labour to do the same task, also once programmed robot will perform better than an experienced human labour. Now a days industry is turning towards computer based monitoring of tasks mainly due to the need for the increased productivity and delivary of the final products with maximum quality. Due to the inflexibility and generally high cost of hard computerization systems lead to the use of industrial robots. In this paper we are introducing a movable robotic arm which is capable of picking up and placing the objects. The soft catching gripper used here handle objects safely.An android based smart phone which has Wi-Fi Module(ESP8266) application is used for the movement of robot. Thus based on the user commands the robot moves and pick and place the objects. The robotic arm used here is similar to a human arm which is programmed to perform the pick and place functions. The remainder of this paper is organized as follows. The section 2 provides information about the existing works. Section 3 gives details of the proposed system. The experimental set up and results were discussed in the section 4.Section 5 concludes the paper.

II. Existing Works

[1]Mohamed.et.al. introduced a Pick and place robotic arm controlled by Computer vision. Here the robot picks the object at a specific orientation only. The gripper used here is a mechanical gripper. So it can't handle the object safely. Objects in a specific orientation is only picked up by the robotic arm.[2] Anush et.al. introduced Design and Fabrication of Movable Rover to Be Used in Library. Here the Rover carry the books from library and deliver this to the destination. The Rover used here can hande objects in any orientation. RFID tags are used to identify the books. This system is capable of doing this specific task only and it□s a line following robot. Each RFID has its own path, and this makes the system

more complex.[3] N F Begum et.al. is designed an Autonomous android controlled robot design using wireless energy. Here the system works according to voice commands or speech deliverd by the user and the robotic arm is capable of picking up the objects of any type and in any orientation. RF technology is used so line of sight is a major constrain in communication.



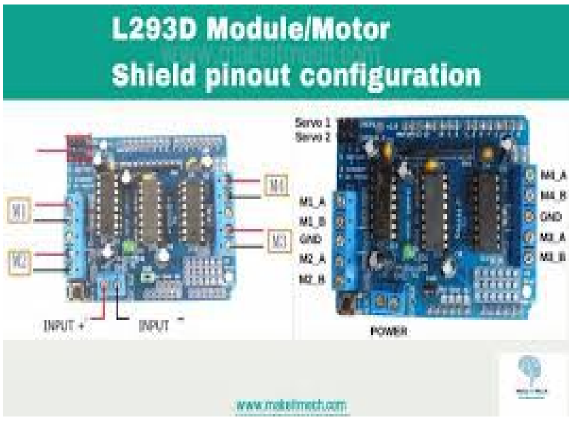
III. Proposed System

The Movable pick & place robotic arm controlled by an Android based smart phone ,which controls the movements of robotic arm through a Wi-Fi module ESP266. Here the robotic arm displaces the object from source to destination safely around a specified range of distance.

For cost effectiveness and reducing harm to the objects, we introduced a robotic arm with better wireless communication technology and soft catching gripper. The soft catching gripper used here reduces the extra pressure to be applied while picking the object thus the objects can be carried without any damage and human effort can be reduced. The robot is controlled remotely using android based smart phone or tablets, so there is no need of complex hardwires to operate this system. This increases the easiness of user. By the use of low power wireless communication technology, the system become more effective and user friendly. Ashly Baby1, Chinnu Augustine2, Chinnu Thampi3, Maria George4,Abhilash A P5,Philip C Jose6 Department of Electronics and Communication Engineering HKCET, Pampakuda Ernakulam, India.

Fig 1 shows the proposed system. It mainly comprised of Arduino atmega microcontroller,Wi-Fi module(ESP01), adafruit motorshild.

The Wi-Fi device are interfaced with the microcontroller. when the user given a command to the microcontroller, it is then checked with the prestored character and if they are same then the robot do the particular operation such as it can move to any direction forward, backward, left, right, arm up, arm down, pick up object and place it. There are four motors are used, two motors are used for the movement of the vehicle and one for the movement of arm and the remaining one for the movement of gripper.

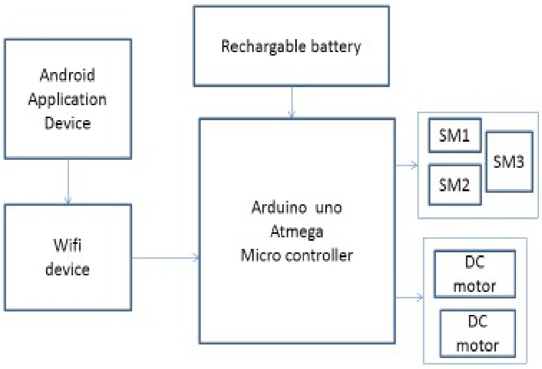


The maximum upward and downward movement of arm and closing and opening of jaw is limited by the mechanical push button type switches. It works on the concept of H-bridge. Wi-Fi control app is used to sending commands to the controller. Wi-Fi control is a basic Universal Remote Control for Wi-Fi enabled serial devices such as Wi-Fi modules connected to a controller. When a button is pressed corresponding to the motor shield

IV. Experimental Setup And Results

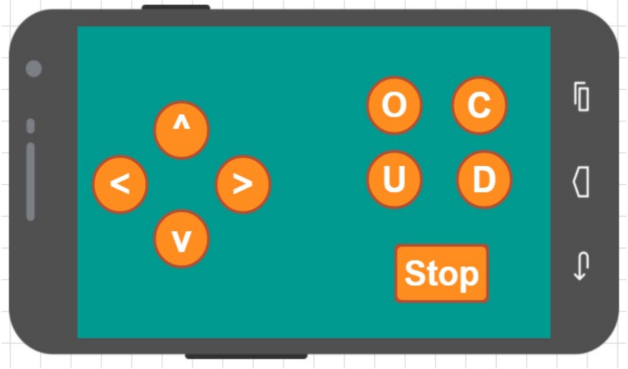
The proposed system is implemented using the Arduino atmega 328P microcontroller. It has 54 input output pins. The operating voltage of mega microcontroller is 5v.The Wi-Fi module and four motors are interfaced with the microcontroller. Each DC motor is connected to the IN1,IN2 and IN3,IN4 of the driver IC.

BLOCK DIAGRAM



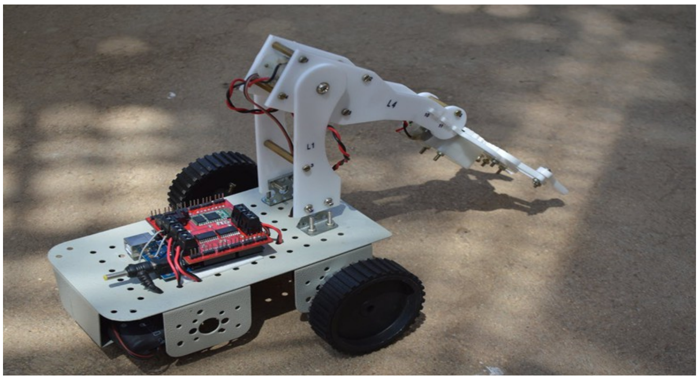
Here the 12V battery provides the over all power supply the motors are connected to the motor shield through the Wi-Fi module ESP8266 the commands are given to the Rover arm to pick& place the object over any direction of overall working of the system. Wi-Fi communication is enabled after power on the system. Once the pairing between the two devices occur, the controller waits for the commands from the user. When the user press a button on the Wi-Fi module corresponding ASCII code is send to the controller. The controller checks this with the prestored value, if they are same then corresponding operation done. For example if the user press U then the operation corresponds to „U is vehicle move forward happens. likewise all other operations are performed. After each command the controller waits for the the next command.

The commands are given by the android based smart phone through the Wi-Fi module here we use Remote XY app to communicate between the user and movable pick & place robotic arm



V. Conclusion

A robotic arm is implemented using arduino to pick and place objects more safely without incurring much damage. The robotic arm used here contain a soft catching gripper which safely handle the object. In the modern era time and man power are major constraints for the completion of a task. By the use of our product the industrial activities and hazardous operations can be done easily and safely in a short span of time. The use of soft catching gripper and low power wireless communication technique like Bluetooth makes our system more effective when compared to other systems. The proposed system is capable of lifting only small weights, by introducing high torque providing motor large weights can be picked. A wireless camera can also be implemented to track the movement of the vehicle and thus it can be used in defence purposes. The range is also a limitation it can be enhanced by using a wireless communication tec



Reference

[1]. Anusha Ronanki , M. Kranthi,"Design and Fabrication of Rover Used in Library", International Journal of
Innovative Research in Science, Engineering and Technology (An ISO 3297: 2007 Certified Organization) Vol. 4, Issue 6, June 2015

[2]. N.F Begum,"Autonomous Android controlled robo design using wireless energy", International Journal of Innovative Research in
Advanced Engineering (IJIRAE) ISSN: 2349- 2163 Issue 2, Volume 2 (February 2015)

[3]. Takashi Yoshimi, Naoyuki Iwata, Makoto Mizukawa and Yoshinobu Ando, Member, IEEE," Picking up Operation of Thin Objects by Robot Arm with Two-Fingered Parallel Soft Gripper", Proceedings of the 2012 IEEE International Workshop on Advanced
Robotics and its Social Impacts, Technische Universität München, Munich, Germany, May 21 - 23, 2012

[4]. B.O.Omijeh,R.Uhunmwangho,M.Ehikhamenle,"Design Analysis of a Remote Controlled Pick and Place Robotic Vehicle",International Journal of Engineering Research and Development e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com Volume 10, Issue 5 (May 2014), PP.57-68

[5]. John Iovine.,"Robots,Androids, and Animations 12 Incredible Projects You Can Build", Second Edition,McGraw- Hill.2002

[6]. Yanjianghuang, ryosukechiba, tamioarai, tsuyoshiueyama and
junota. ,"Integrateddesign of multi-robot system for pickand- place tasks",

[7]. Sungwookmoon ,youngjinkim, ho junmyeong , changsookim, namjucha,and dong hwankim . ,"Implementation of smart phone environment

[8]. ATMELATmega48A/PA/88A/PA/168A/PA/328/P [Datasheet] 2 Atmel-8271I-AVR-ATmega-Datasheet10/2014.

[9]. SGS Thomson Microelectronics L293D - L293DD [Datasheet] push-pullfour channel driver with diode .June 1996.

[10]. Fairchild semiconductor KA78XX/KA78XXA 3- Terminal 1A Positive Voltage Regulator Data sheet.2001 Fairchild Semiconductor Corporation.

Efficient edge detection algorithm for blurred images

Mrs.C.Suganya,
Assistant Professor,
Department of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Ms.C. Akshaya,
PG Student,
Department of Computer Science and Engineering,
Perunthalaivar Kamarajar Institute of Engineering and Technology,
Karaikal-609603.

Abstract- Edges characterize object boundaries and are therefore useful for segmentation, registration, and identification of objects. Edge detection is the technique used for image segmentation and data extraction in areas such as image processing, computer vision, and machine vision. This paper focuses on enhancing a blurred image captured on occasions like bad weather conditions or captured during motion. Areas of high frequency is extracted from the blurred image and then processed. Consequently, the high-frequency image is divided into nine sub regions, based on a sliding window, and the rich edge region index of each region is determined. Then, the region with the richest edge information is extracted. Finally, the extracted edge region, instead of the entire motion blurred image, is used to estimate the blur kernel with L0-regularized intensity and gradient prior, and the blurred image can be restored. Experimental results show that the proposed method can improve the recovery efficiency while ensuring the recovery quality as well.

Index Terms—**Image processing, Image restoration, Image quality, Motion blurred image**

I. INTRODUCTION

The purpose of detecting sharp changes in image brightness is to capture important events and changes in properties of the world. Use of an edge detection algorithm to an image may significantly reduce the amount of data to be processed and may therefore filter out information that may be regarded as less relevant. If the edge detection step is successful, the subsequent task of interpreting the information contents in the original image may therefore be substantially simplified. Motion blur in images is a common phenomenon and the restoration of motion blurred images has always been a research hotspot in the computer vision field. The combination of denoising and edge detection with the estimation of motion results in an energy functional incorporating fidelity- and smoothness-terms for both the image and the flow field.

Various operators are available for edge detection namely Roberts, Prewitt, Sobel etc. Most of these partial derivative operators are sensitive to noise. Use of these masks resulted in thick edges or boundaries, in addition to spurious edge pixels due to noise. Laplacian mask is highly sensitive to spike noise. Use of noise smoothing became mandatory before edge detection, specifically for noisy images. But noise smoothing, typically by the use of a Gaussian function, caused a blurring or smearing of the edge information or gradient values.

II EDGE DETECTION

More details are required to improve the motion blur. Firstly the edges are extracted by means of an efficient edge detection algorithm. Part of an image has to be taken instead of an entire image

There are 3 main process for edge detection, (i) *Filtering*- Filtering can be used for improving the performance of edge detector. However more filtering may reduce the strength of the edges. (ii) *Enhancement*- In order to facilitate the detection of edges, it is essential to determine changes in intensity in the neighborhood of a point. Enhancement emphasizes pixels where there is a significant change in local intensity values and is usually performed by computing the gradient magnitude. (iii) *Detection*- We only want points with strong edge content. However, many points in an image have a nonzero value for the gradient, and not all of these points are edges for a particular application. Therefore, some method should be used to determine which points are edge points. Frequently, thresholding provides the criterion used for detection

Algorithm:

Step 1: Relief edges are defined as the zero crossings of the normal curvature in the direction perpendicular to the edge.

Step 2: The edge direction is estimated for every point by fitting a step edge model to the surface.

Step 3: Given the edge directions, the precise edge localization is obtained

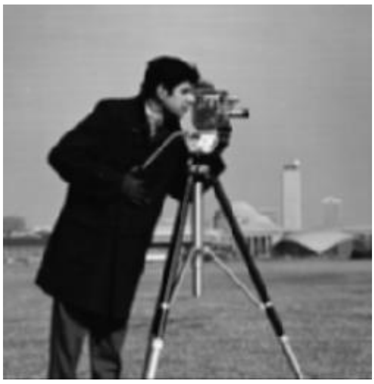
Step 4: Sliding window is applied and high frequency surface is scanned.

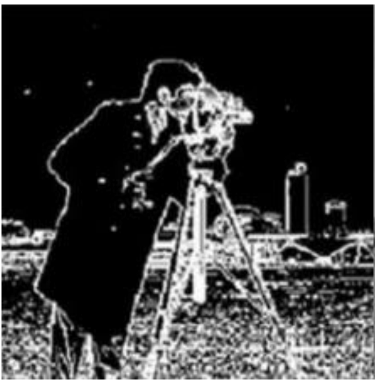
Step 5: The high frequency regions are further sub divided and then restored.

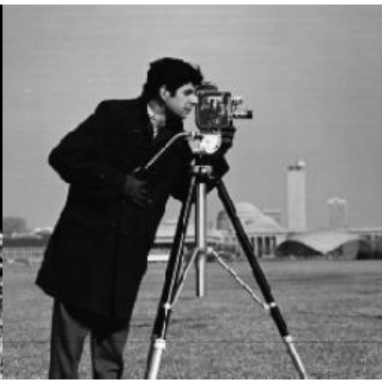
III IMAGE RESTORATION

Image restoration recovers the high frequency information in an image that was removed by the low-pass degradation system. Therefore, in following a learning approach to restoration, the mapping between low- and high-frequency information in an image needs to be established during training. During restoration the low-frequencies in the available noisy and blurred data are mapped with the use of a codebook to high frequencies, which when added to the available data provide an estimate of the original image. In designing the codebook, a straightforward decomposition of an image into low- and high-frequency components is first performed.

IV EXPERIMENTAL RESULTS







Original blurred image

High frequency layer

Restored image

The recovery effect with the proposed edge region is significantly better than the existing one. The main reason is that the rich edge region contains more information than the non-rich edge region about the pixel intensity and gradient, which are essential for blur kernel estimation. The restoration effect with the rich edge region is similar to that with the entire image, while the recovery time decreases significantly. This is mainly because the proposed method only needs part of the image in the blur kernel estimation process, which greatly reduces the calculation.

V CONCLUSION

In this paper, deblurring of an image is performed using efficient edge detection algorithm. The method made three main contributions. First, the coefficients of the gray-level co-occurrence matrix were analyzed and an index representing the amount of image edge information was presented, which helped extract the rich edge region. Second, the high-frequency layer was extracted to compute the coefficients of the gray-level co-occurrence matrix. Third, a sliding window was used to divide the high-frequency layer image, and the rich edge region index of each region was calculated. The region with the edge information could replace the entire blurred image for blur kernel estimation and recovery. This greatly reduced the recovery time. Experimental results, including the visual effect of the image restoration using the algorithm proposed.

REFERENCES

[1] Minghua Zhao, et.al., “Restoration of Motion Blurred Images Based on Rich Edge Region Extraction Using a Gray-Level Co-Occurrence Matrix”, IEEE conference on image processing, DOI 10.1109/ACCESS.2018.2815608, 2018.

[2] A. Levin, Y. Weiss, F. Durand, W. T. Freeman, “Understanding and evaluating blind deconvolution algorithms”, IEEE Transactions on Pattern Analysis & Machine Intelligence, vol. 33, no. 12, pp. 2354-2367, 2011.

[3] A. Levin, Y. Weiss, F. Durand, W. T. Freeman, “Understanding and evaluating blind deconvolution algorithms”, IEEE Conference on Computer Vision & Pattern Recognition, vol. 8, no.1, pp. 1964-1971, 2009.

[4] A. Gupta, N. Joshi, C. L. Zitnick, M. Cohen, B. Curless, “Single Image Deblurring Using Motion Density Functions”, European Conference on Computer Vision, vol. 6311, pp. 171-184, 2010.

[5] L. Zhong, S. Cho, D. Metaxas, S. Paris, J. Wang, “Handling Noise in Single Image Deblurring Using Directional Filters”, IEEE Conference on Computer Vision & Pattern Recognition, vol. 9, no. 4, pp. 612-619, 2013.

[6] L. Xu, S. Zheng, J. Jia, “Unnatural L0 Sparse Representation for Natural Image Deblurring”, IEEE Conference on Computer Vision & Pattern Recognition, vol. 9, no. 4, pp. 1107-1114, 2013.

[7] D. Krishnan, T. Tay, R. Fergus, “Blind deconvolution using a normalized sparsity measure”, IEEE Conference on Computer Vision & Pattern Recognition, vol. 42, no. 7, pp.233-240, 2011.

[8] J. F. Cai, H. Ji, C. Liu, Z. Shen, “Blind motion deblurring from a single image using sparse approximation”, IEEE Conference on Computer Vision & Pattern Recognition, pp. 104-111, 2009.

[9] R. Fergus, B. Singh, A. Hertzmann, S. T. Roweis, W. T. Freeman, “Removing camera shake from a single photograph”, ACM Transactions on Graphics, vol. 25, no. 3, pp. 787-794, 2006.

Multi-Role Unmanned Ground Vehicle for Rescue and Defense Applications

Ms.M. Keerthana
UG Scholar,
Department of Electronics and Communication Engineering,
V.R.S. College of Engineering and Technology,
Arasur-607017, Tamil Nadu.

Ms.A. Nilofarnisha
UG Scholar,
Department of Electronics and Communication Engineering,
V.R.S. College of Engineering and Technology,
Arasur-607017, Tamil Nadu.

Mr.V. Thiyagarajan
Associate Professor,
Department of Electronics and Communication Engineering,
V.R.S. College of Engineering and Technology,
Arasur-607017, Tamil Nadu.

Abstract - Nowadays the world is very insecure due to various problems like terrorism, natural disasters, emergency health situations and surveillance. Valuable lives are being lost in various situations due to human negligence when carrying out rescue or emergency operations. Even though when our security forces are tireless working to save us every day, we still have problem to entirely secure ourselves in different situations. To counter these issues we propose a project. Our project is a multi-role capable unmanned ground vehicle. The current types of unmanned ground vehicles are designed for doing only one specific task like bomb detection, live human detection, border alert system, assisting robot etc., but our unmanned ground vehicle is designed to undertake multiple tasks. The robot is equipped with a PIR sensor to detect live human, metal detector for bomb detection, detect the obstacle by capturing the border alert using camera. Raspberry Pi 2 is used to control the Unmanned Ground Vehicle (UGV) and is the core of UGV and DC motors attached to perform forward and reverse movements. This UGV can detect live human and bomb detection, monitor condition of the place like temperature and presence of natural gas. A camera is attached with this UGV with which it can observe the condition of the border system. It also contains a coil gun with which it can attack enemy within a range of 10 fit and has also obstacle detector to protect itself. By implementing a mix of modular design, simple and cheap circuitry we can develop an effective and reliable multi- role capable unmanned ground vehicles.

Keywords: Raspberry Pi, Python, PIR Sensor, Open CV, Surveillance.

I. INTRODUCTION

An unmanned ground vehicle (UGV) is being developed day by day in different applications like military and civilian operations, surveillance, border patrolling, law enforcement, hostage situation, and police for some specific mission to detecting and diffusing bombs. A timely rescue can only save the people who are buried and wounded due to a disaster. In such situations, rescue system must take fast decisions under pressure, and try to get victims to safe location at their own risk. The rescue system must collect the location information and status of victims as quickly as possible so that medication and fire-fighters can enter the disaster prone area and save people. All these works are performed mostly in very dangerous and risky situations by human and trained dogs. Detection by rescue workers becomes time consuming and due to the vast area that gets affected it becomes more difficult. So the project proposes a rescue robot that moves in a disastrous area and helps in identifying the live people and rescue operations. We are introducing an UGV which senses the movement in border area without manpower and launches its gun towards the target. A unique Passive Infrared sensor is used in the project which emits infrared rays to detect humans. As live human body emits thermal radiation it is received and manipulated by the PIR sensor to detect humans. The real time bomb sensor is not used because of the variable composition of bomb material, a metal sensor or magnetic sensor can be used as a proto-type and can be replaced by a real bomb sensor if used practically widely for the purpose.

II. PROPOSED SYSTEM

The objective of this project is to implement automation of unmanned ground vehicle with the help of raspberry pi 2B. The project proposes a multi-role unmanned ground vehicle that moves in the battle field and helps in identifying the live people those are injured and performs rescue system operations and monitoring border alert system. There is a communication link between control unit and UGV unit via Zig-Bee Link. One raspberry pi 2B model, a wireless camera, array of sensors, motor driver circuitry to control and drive the motors and Zig-Bee modem Circuitry to transmit and receive signal being send by UGV unit. Then the sensors (PIR, Gas, Metal, Obstacle), motors, coil gun were connected according to the design. Here the Zig-Bee module used for receiving the transmitted signal from the transmitter.

Outputs of sensors are connected to Raspberry Pi processor shown in figure 1 then outputs are processed and according to sensors' outputs functions are performed. Also information is transmitted to control room unit shown in figure 2 via ZigBee transceiver for monitoring purpose. Images are captured by wireless camera which is used to detect enemies crossing border. Based on that coil gun is targeting enemy and hit him as well as images are transmitted to control room unit for defense applications.

II.1 Unmanned Ground Vehicle

The vehicle can be operated autonomously i.e (able to work without human). It is widely used where inconvenient, hazardous or difficult to handle the situation by human operators. It has the ability to track the path, gather user about the environment, period of working can be extended without the help of operators. They can also repair themselves without outside assistance. They can be widely used in Defense applications, Agriculture, Industries, etc,. It can able to monitor and self-restrained machine.

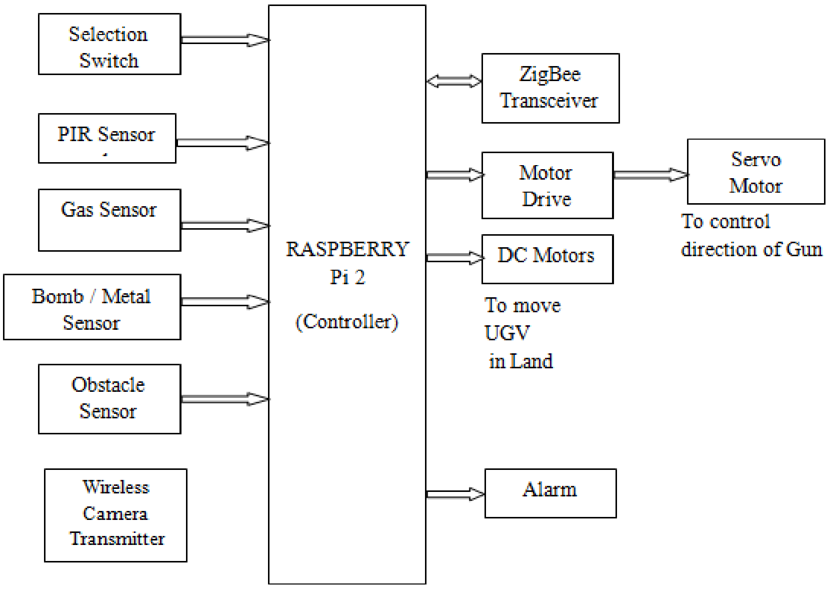


Figure 1: Block diagram of Proposed Unmanned Ground Vehicle

II.2 Control Unit

The control unit compromises of a PC, GUI interface software, a Zig-Bee Rx-Tx duplex communication modem, a level converter which converts host computer control signal to Zig-Bee compatible signal and a driver interface card. A wireless RF receiver is used to receive the footages send by the camera placed on the UGV unit to visualize the live video of the place where the UGV is present. Using a driver interface card, the can be seen on the host PC or can be directly seen on a television without using any interface card. Though the PC does not understand the signal received by Zig-Bee, we use Level-Converter in between PC and modem to change the level of signal and make the signal PC acceptable.

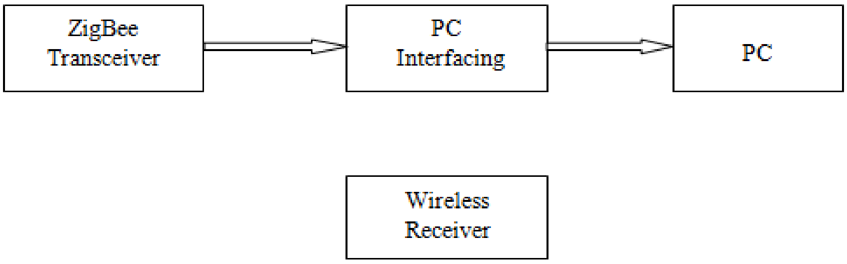


Figure 2: Control Room Unit

III. HARDWARE & SOFTWARE IMPLEMENTATIONS

3.1 Hardware Requirements:

Raspberry Pi 2B
ZigBee Transceiver
Wireless Camera
Servo Motor
DC Motor
PIR Sensor
GAS Sensor
Metal Sensor

Obstacle Sensor
Buzzer

3.2 Software Requirements:

Python Language
Raspbian OS

3.3 Raspberry Pi 2:

The raspberry pi 2 is core kit which replaces the personal computer and does the process very efficiently. The method includes vital hardware components and software. It is a small sized single board computer. The Raspbian OS installed in the Raspberry pi 2B kit and the necessary library functions are installed using python libraries.

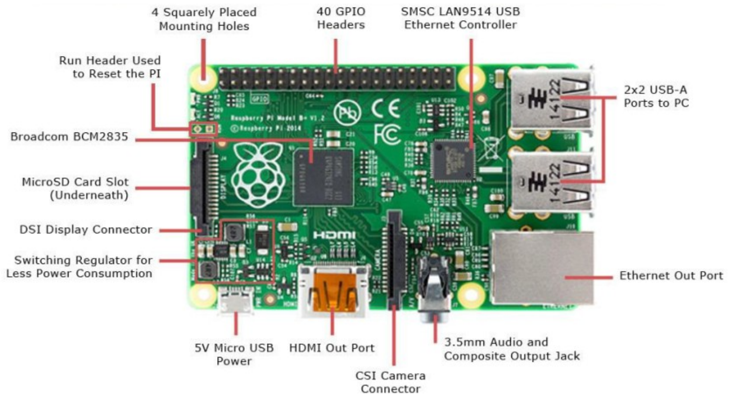

4 Squarely Placed Mounting Holes
40 GPIO Headers
SMSC LAN9514 USB Ethernet Controller
Run Header Used to Reset the PI
2x2 USB-A Ports to PC
Broadcom BCM2835
MicroSD Card Slot (Underneath)
DSI Display Connector
Switching Regulator for Less Power Consumption
Ethernet Out Port
5V Micro USB Power
HDMI Out Port
CSI Camera Connector
3.5mm Audio and Composite Output Jack

Figure 3: Overview of the Raspberry Pi 2.0 B

3.4 Raspbian OS - Noobs:

Among all operating system such as Risc OS, Chromium OS, Angstorm Linux, Pidora, Gentoo, Raspbian is the best one for Raspberry. It is feasible for working and also free operating system available in the website. Raspbian also has types as wheezy, Jessie, noobs. We prefer noobs because it improves the performance and flexibility, particularly as regards the control of the system processes, fast, pre-programmed, high capacity and as with any update, there are also numerous bug fixes and tweaks.

3.5 Python:

It is high level programming language which allows coders to express their ideas in fewer lines when compared other programming languages like C, C++, Java. It also had large number of packages and also used to combine software with hardware. Python can be executed directly by the system without compiling it. So the execution time is very less when compare with other programming languages.

3.6 ZigBee Transceiver:

It is used to send and receive data between UGV and the control unit. Zigbee is a digital wireless communication protocol. It is a very low power communication technology. Zigbee is a very versatile communication technology. XBee and XBee-PRO Modules were engineered to meet Zigbee/IEEE 802.15.4 standards and support the unique needs of lowcost, low-power wireless sensor networks. The modules operate within the ISM 2.4 GHz frequency band and are pin-for-pin compatible with each other.

3.7 Power Supply Unit:

In this circuit, the required power is 5V for micro-controller and motor driver IC, 3.3V for Zig-Bee and 6V for motors. Thus, the Power supply is given to the circuit by 230V AC for Control unit and via 6V battery in UGV unit. The L293D motor driver IC is designed to provide a bidirectional drive currents of up to 600mA at voltages from 4.5 V to 36 V. Devices are designed to drive inductive loads such as relays, dc and bipolar stepping motors.

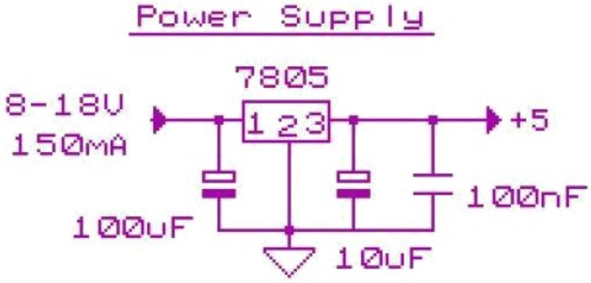


Figure 4: Regulated DC Power Supply

3.8 DC Motor:

DC Motors can rotate in two directions depending on polarity of the battery connected to the motor. Both the DC motor and the battery are two terminal devices that have positive and negative terminals. In order run the motor in the forward direction, connect the positive motor wire to the positive battery wire and negative to negative. However, to run the motor in reverse just switch the connections; connect the positive battery wire to the negative motor wire, and the negative battery wire to the positive motor wire. An H-Bridge circuit allows a large DC motor to be run in both directions with a low level logic input signal. Here we use four DC motors for moving UGV.

3.9 Servo Motor:

A servomotor is a rotary actuator or linear actuator that allows for precise control of angular or linear position, velocity and acceleration. It consists of a suitable motor coupled to a sensor for position feedback. It also requires a relatively sophisticated controller, often a dedicated module designed specifically for use with servomotors. Servos are controlled by sending an electrical pulse of variable width, or pulse width modulation (PWM), through the control wire. There is a minimum pulse, a maximum pulse, and a repetition rate. Servo motors can usually only turn 90 degrees in either direction for a total of 180 degree movement. The motor's neutral position is defined as the position where the servo has the same amount of potential rotation in the both the clockwise or counter-clockwise direction. This motor is used to target the coil gun.

3.10 Wireless Camera:

To visualize the live environment around the robot, a wireless mini RF camera is used. There are two units of Camera, receiving unit and transmitting unit. Transmitting unit contains of camera with a RF transmitter and Receiving unit compromises with an RF antenna and a signal processing driver unit. In addition to that if we use PC to watch the footages, an additional Driver Interface Card will come into the picture to change the signal level to PC compatible.

Figure 5: Wireless Mini Camera

3.11 Sensors used in UGV:

3.11.1 PIR Sensor:

As live human body emits thermal radiation it is received and manipulated by the PIR sensor to detect humans. PIR sensors are passive infrared sensors. They detect change in the heat and this can be used to detect movement of people. It has digital output and can be directly given to Integrated Intelligent Research (IIR) the digital pins and no ADC is needed. It operates at 5V DC. The PIR (Passive Infra-Red) Sensor is a pyroelectric device that detects motion by measuring changes in the infrared (heat) levels emitted by surrounding objects. This motion can be detected by checking for a sudden change in the surrounding IR patterns. When motion is detected the PIR sensor outputs a high signal on its output pin. This logic signal can be read by a microcontroller or used to drive a transistor to switch a higher current load. Detection ranges up to 20 feet away.

Figure 6: PIR Sensor

3.11.2 METAL Sensor:

A Bomb/Metal sensor detects the presence of suspected material in Rescue operation. The real time bomb sensor is not used because of the variable composition of bomb material, a metal sensor or magnetic sensor can be used as a proto-type and can be replaced by a real bomb sensor if used practically widely for the purpose.

3.11.3 GAS Sensor:

MQ05 gas sensor has been used in the UGV. It will sense if there is any unusual gas present or not. If detects any gas, it will send the data to the microcontroller.

3.11.4 Obstacle Detector:

An obstacle detector sensor implemented to the UGV to prevent any damage to the body of the UGV as well finding border line. If it found any obstacle very near to the body of the UGV, it will prevent the forward movement of the UGV.

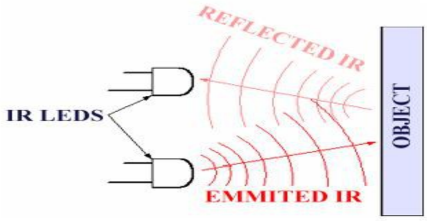


Figure 7: Object Detection Using IR Light

3.12 Coil Gun:

The coil gun contains two parts.

Charge Control Part:

To shoot through the coil gun high voltage need to boost the coil. To supply high energy two 400v 220µF capacitor has been used. To charge the capacitor a high frequency inverter has been used.

Coil:

To shoot through the coil gun an electro magnet need to produce. 20ft long insulated wire used to make the coil to produce the elector magnet. Coil gun able to shoot any object within the range of 10 feet.

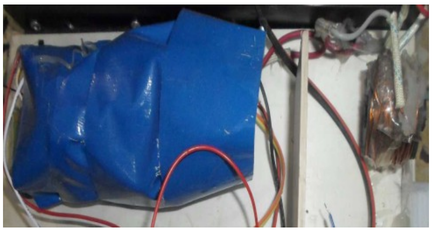


Figure 8: Coil Gun Circuit

3.13 Buzzer:

This buzzer is an electromagnetic type audio signaling device, which has a coil inside which oscillates a metal plate against another, which when given voltage difference produces sound of a predefined frequency. You must be aware of such sounds of buzzer like BEEP sound in many appliances.

Figure 9: Buzzer

IV. APPLICATIONS

The application of the use of unmanned ground vehicle are immense some of the real applications of the vehicle are as follows

a. Bomb detection and handling
b. Surveillance
c. Multi-role capacity

d. Border alert system
e. Disaster situations

V. CONCLUSION

This system demonstrates the use of unmanned ground vehicle designed for multi-role capabilities like the robotic arm for metal detector to detect bombs, surveillance, live human detection, border alert system etc. The unmanned system is a game changing technology that everyone is betting the future to be filled with unmanned system. We have already seen a lot of unmanned systems coming into our social lives like the drones, serving food etc., and this is just the beginning of a new revolution our day to day lives. This project sets a example of the current trend of the use of unmanned system in the military defense applications.

REFERENCES

1. A. Mugan, A. bner, A. Apak, C. Dikilita, H. Heceoglu , V. Sezer, Z. Ercan,and M. Gokasan "Conversion of a conventional electric automobile into an unmanned ground vehicle (UGV)", Proceedings of the IEEE International Conference on Mechatronics, 2012.
2. A. Mohebbi, M. Keshmiri,S. Safaee, and S. Mohebbi, "Design, Simulation and manufacturing of a Tracked Surveillance Unmanned Ground Vehicle", Proceedings of the IEEE International Conference on Robotics and Biomimetices, pp.14-18; 2010.
3. Md. Ajijul bin zabbar, Nafiz ahmed chisty "Design & mplementation of an Unmanned Ground Vehicle Surveillance Robot" International Journal of Electrical and Electronics Engineering (IJEEE); 2016.
4. Hardeep Pal Sharma; Guna sekar.C.H "Live Human Detecting Robot for Earthquake Resque Operation", Vol. 2, Issue 01, June 2013.
5. Sivasoundari, S.Kalaimani, M.Balamurugan: "Wireless Surveillance Robot with Motion Detection and Live Video Transmission"," *International Journal of Emerging Science and Engineering (IJESE)"* ISSN: 2319–6378, Volume-I, Issue-6 April 2013.
6. Trupti B. Bhondve, Prof.R.Satyanarayan, Prof. Moresh Mukhedkar: "Mobile Rescue Robot for Human Body Detection in Rescue Operation of Disaster", "*International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering",* Vol. 3, Issue 6, June 2014.
7. Jai rajesh.P, Dhanasekar J, V.G. Vijaya "multi-role unmanned ground vehicle for bomb detection and surveillance" , "*International Journal of Pure and Applied Mathematics"* Volume 116, 2017.
8. An autonomous wireless sensor network deployment system using mobile robots for human existence detection in case of disasters Ad Hoc Networks 13 (2014) 54–68.
9. Alive human body detection system using an autonomous mobile rescue robot India Conference *(INDICON)*, 2011 Annual IEEE.

Design and Implementation of Anti-Collision system to prevent Train Accident Dynamically Using Embedded System

Ms. S. Devika,
Assistant Professor,
Department of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Mrs. M. Vaidehi
Professor,
Department Of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Mrs. M. Mary Amala Jenni,
Assistant Professor,
Department Of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

***Abstract* - Railway is the most popular and friendly transportation system of the largest part of the cities in the world. Train is widely used for comfortable and safe journey in a reasonable fare. People from different professions can effort it. Almost 10,000 billion freight tonne-Kilometers and more than 5 billion Passengers of rail transport have been travelled around the world per years. The railway transportation system plays an important role for business as well as for leniency and safe travelling in modern life. But at every turn, the train is facing unexpected situation in travelling because of wrong signal, wrong track switching, insecure level crossing etc. for which collision have been occurred. As a result, lot of damages has been done in economic sector with lot of causalities which affect our progress. But we can avoid this unexpected collision and take prevention from the accident dynamically by using the collision detection technology which can be made by ultrasonic sound with a special embedded system. By using this technology can detect the obstacle and gradually slow down the speed by initiating the air brake to stop the train before the collision takes place.**

***Key Words*: Ultrasonic Sensor, Microcontroller board, Control Device, Alarm, DC Servo motor, Embedded System.**

1. INTRODUCTION

Railway is the most popular and friendly transportation system in the world. Rail transports are facing major challenges in our day to day life. Rail transport systems first appeared in England in 1820s. From 1820-2016 many evolution is occurred. At present railways is one of the most widely used transportation system in the world. Approximately 10,000 billion freight tonne-Kilometres are travelled around the world every year and more than 5 billon passengers travelled per year as per Railway statistic report. Economists have argued that the existence of modern rail infrastructure is a significant indicator of a country's economic advancement. But till now railway transportation system are not safe. Many countries' railway faces many collisions during travelling in every year as a results happened lot of damages and casualties. But if we add Anti-Collision Technology (ACT) in railway then we can prevent any types of collision. It is an innovative technology which can be detect collision object from specific distance of train and avoid collision dynamically and efficiently by using ultrasound and embedded system.

2. TRAIN ACCIDENT

The train accident is one of the most dangerous accidents ever. The common reason of the train collisions are malfunctioning train signals or lights, failing mechanics, safety gates not in place ,crossings that are unprotected, negligence of train conductor and lack of awareness of the people.

2.1 Train Collision in Different Countries

1. Every year in many countries around the world occurred train accidents. Here are some accidents have been highlighted.
2. 8 December 2010 – Bangladesh – Two passenger trains are in a head-on collision near Narsingdi. Nineteen people are killed.
3. 20 May 2011 – South Africa – 857 people are injured, 25 seriously, when a rear-end collision occurs at Soweto.
4. 23 July 2011 – China – Wenzhou train collision – Due to signal failure, a high- speed train rear-ends a stopped high-speed train at a speed of 99 km/h (62 mph) near Wenzhou in the province of Zhejiang, killing 40 people and injuring at least 192.
5. 11 January 2012 - 5 persons were killed and 9 others, including a child, injured in a collision between the Delhi-bound Brahmaputra Mail and a stationary goods train.
6. 22 May 2012 - The Hubli-Bangalore, Hampi Express collided with a goods train near Penukonda in Andhra Pradesh. 14 people were dead and 35 were injured in the collision.
7. 24 July 2014 – India – Medak district bus-train collision – A school bus is hit by Nanded Passenger train at an unmanned railway level crossing in Masaipet village of Medak district. 18 bus passengers died including 6 students.
8. 15 September 2016- A Karachi bound express train has collided with a stationary freight
   train in Pakistan's central Punjab region, killing at least 6 people and injuring more than 150.
9. 3 November 2016 – Atleast 20 people were killed and nearly 70 injured when zakaria Express collided into stationary coaches of Fareed Express at a railway station in Karachi. The engine of one train was completely destroyed.
10. **Utkal Express derailment, Aug 18, 2017.** At least 23 people were killed and over 40 others injured when 14 coaches of Puri-Haridwar-Kalinga Express train derailed in Khatauli in Uttar Pradesh's Muzaffarnagar district.
11. **Meerut-Lucknow Rajya Rani Express derailment, April 15, 2017.**
    Ten people were injured when the express train derailed near Rampur in Uttar Pradesh. The derailment happened near a bridge over the Koshi river. UP Chief Minister Yogi Adityanath announced Rs 50,000 compensation to those seriously

injured and Rs 25,000 to people with minor injuries.

12. **Jagdalpur-Bhubaneswar Hirakhand Express derailment, Jan 22, 2017.**
Twenty-seven people were killed and 36 others were injured when nine coaches of the express train derailed in Andhra Pradesh's Vizianagaram district.

13. **Kalindi Express derailment, Feb 20, 2017.**
The engine and the three coaches of the Delhi-bound Kalindi Express was derailed at the Tundla Junction in Uttar Pradesh. The derailment happened when the train rammed into a freight train from the back.

14. **Ujjain train blast, March 3, 2017.**
Eight people were injured, two of them seriously, in an explosion in the Bhopal-Ujjain passenger train near Jabdi station in Madhya Pradesh. The state government had called it a terrorist attack.

15. **Train rams into ambulance in Bengaluru, March 17, 2017.**
Four women were killed when a passenger train rammed into an ambulance at an unmanned level crossing at Mannekote-Talaka road in Karnataka's Chitradurga district. The ambulance driver misjudged the speed of the approaching train and tried to cross the unmanned level crossing.

16. **Mahakaushal Express derailment, March 30, 2017.**
A total of 52 passengers were injured when the Mahakaushal Express derailed in Uttar Pradesh. The train, which runs between Jabalpur in Madhya Pradesh and Hazrat Nizamuddin in Delhi derailed near Kulpahar station.

17. **Goods train derailment in West Bengal, April 9, 2017.**
The engine of a goods train derailed between Madpur and Jakpur stations in West Bengal. The derailment had affected train services. However, there was no casualty.

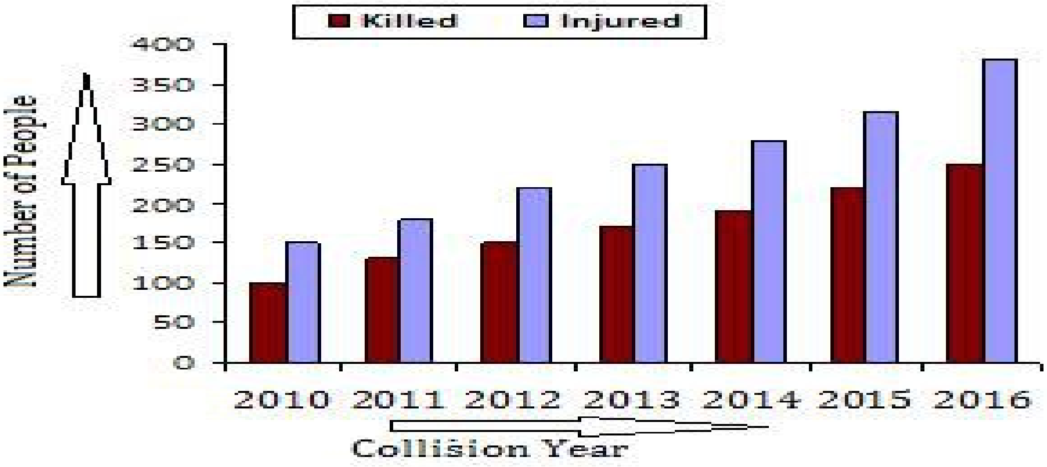


Chart-1: Survey chart on train collision.
Chart-1 represents approximate quantity of killed people and injured people in last seven years train collision around the world.

3. PROPOSED SYSTEM

This proposed Anti-Collision System (ACS) will have the significant impact on the railway safety. This Anti-Collision System (ACS) is made by ultrasonic sensor with microcontroller depended embedded system which can work on emergency air brake to control a high speedy train. Ultrasonic sound is used to measure the distance using sensor. When it detects any obstacle in front of the train then it runs the alarm with a red signal. If the system is in automatic mode then it activates the automatic brake otherwise it works according to Loco pilot's decision. If there is no obstacle found then it shows the green clearance signal.

A flowchart of our proposed anti-collision system is shown in Fig-1.

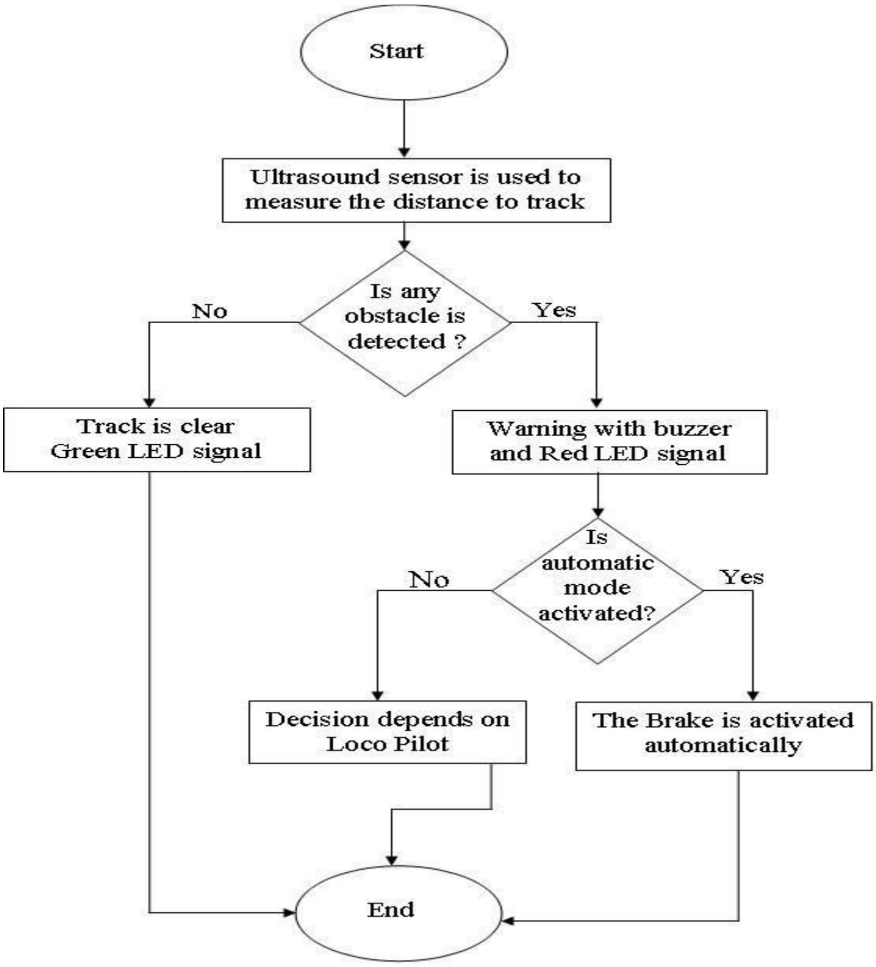

Start
Ultrasound sensor is used to measure the distance to track
Is any obstacle is detected ?
No
Yes
Track is clear Green LED signal
Warning with buzzer and Red LED signal
Is automatic mode activated?
No
Yes
Decision depends on Loco Pilot
The Brake is activated automatically
End

Fig-1: Flowchart of proposed Anti Collision System.

This flowchart (Fig-1) represents our proposed anti-collision system (ACS) working processes. There is an Ultrasound device which always check obstacle in front of the train and measured distance from sensor end to track. If there is no obstacle then it will show green signal and display track clearance message. If obstacle is detected then it will warning with buzzer and red signal and display obstacle distance from the train. In this Anti-Collision Device (ACD) there is a switch to select automatic or manual mode. If an automatic mode is activate then the emergency brake active automatically and control the train. On the other hand, if the manual mode is active then it will detect an obstacle and warn to responsible loco pilot to activate the brake for control the train manually.

4. SYSTEM SETUP

In this system Fig-2 we have used a microcontroller ATMega328p, Ultrasound sensor, Buzzer, Servomotor, Control Device (LCD Display, LED light (Red, Green) and switch).

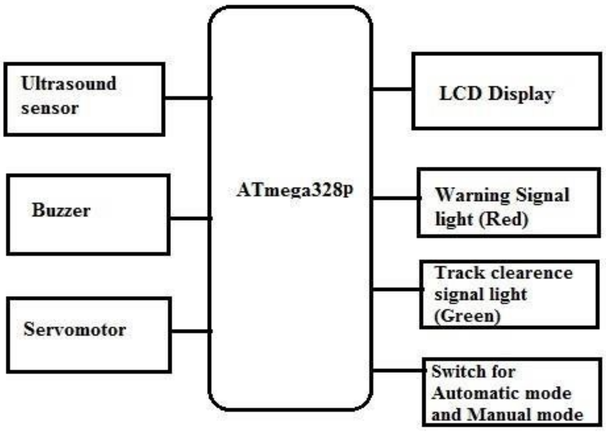

Ultrasound sensor
Buzzer
Servomotor
ATmega328p
LCD Display
Warning Signal light (Red)
Track clearence signal light (Green)
Switch for Automatic mode and Manual mode

Fig-2: Anti Collision System module.

4.1 Ultrasound Sensor:

Ultrasound sensor is a high frequency sound sensor. It produces frequency higher than 20 kHz. Which is non hearable for human being. Usually ultrasound transducer devices convert the sound into ultra sound. Ultra sound transmits and receive signal with transducer device where the speed of ultra sound signals depends on the environment shown in Fig-3. It will enable to find an object into selected range. Its count an object as an obstacle if the object like as humans, vehicles, big trees or more than bigger object. In air sound speed 345 m/s approximately, in water the speed of ultra sound is 1500 m/s approximately and in metal the speed of ultra sound is 5000 m/s approximately.

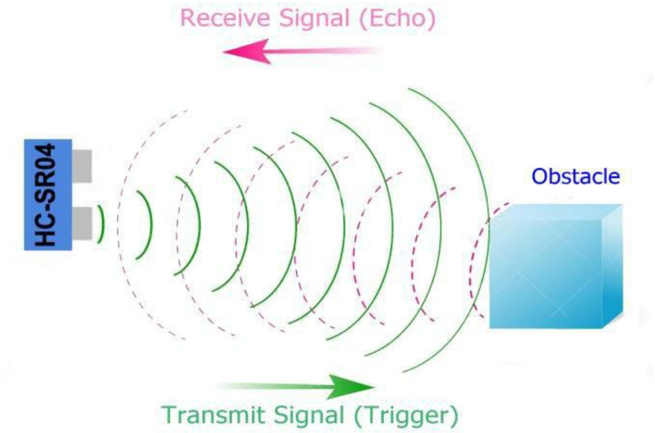


Fig-3: Receive and Transmit signal between ultrasound and obstacle.

memory with read-while-write capabilities, 1 KB Erasable Programmable Read Only Memory (EEPROM), 2 KB Static Random Access Memory (SRAM), 23 general purpose I/O lines, 32 general purpose working registers, three flexible timer/counters with compare modes, internal and external interrupts, Universal Synchronous/Asynchronous Receiver Transmitter (USART), a byte-oriented 2-wire serial interface, SPI serial port, 6-channel 10-bit A/D converter (8-channels in TQFP and QFN/MLF packages), programmable watchdog timer with internal oscillator, and five software selectable power saving modes. The device operates between 1.8-5.5 volts. The device achieves throughput approaching 1 MIPS per MHz.

4.2 Servo Motor:

A servomotor is a rotary or linear actuator that allows for specific control of angular or linear position with velocity and acceleration. Servomotors are not a specific class of motor although the term servomotor is used to refer a motor which is suitable for use in a closed -loop control system. In this collision avoidance system a servomotor works for turning air brake (automatic brake) at emergency situation shown in Fig-4.

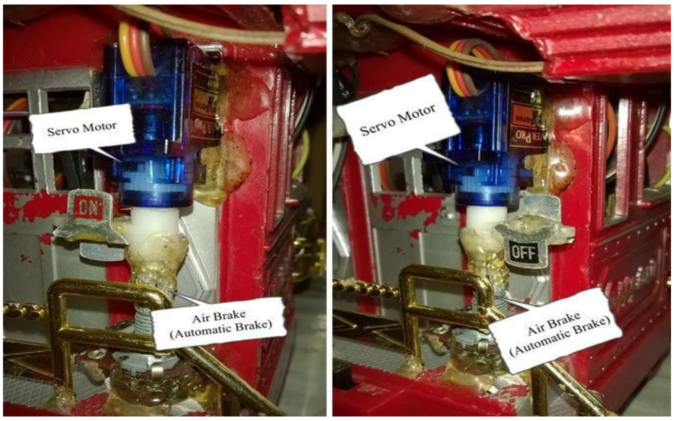


Fig-4: Working system of servo motor on air brake.

4.3 Microcontroller ATMega328p:

Microcontrollers are used in automatically controlled products and devices, such as automation machine control systems and other embedded systems. The ATmega328p is a single-chip microcontroller created by Atmel in the mega AVR family. The Atmel 8-bit AVR RISC-based microcontroller combines 32 KB In System Programmable (ISP) flash

4.4 Automatic Air Brake

Air brake is the standard, safe and effective braking system with compressed air. It is also known as Westinghouse Air brake. Air brake used by railways all over the world. It has an air reservoir and triple valve. But some modern air brake has two or three air reservoir tank. An air reservoir charged the cylinder with triple valves. When a train active the air brake then compressed air released from the reservoir and reached to brake cylinder through the pipe line. An air brake compressor is usually capable of generating a pressure of 90 psi (620 KPa). All over the world, air brake is used as an automatic brake in emergency situation and can reduce the speed rapidly.

4.5 Control Device:

Control device is a part of anti-collision and embedded system. This device specially designed for loco pilot (which shown in Fig-5 and Fig-6). Control device has various types of components. A loco pilot gets update information of the track’s current situation from LCD display. There is a switch to select automatic mode or manual mode. An automatic mode detects collision object, give warning and at last active automatic brake for reducing speed up to zero and stop the train. On the other hand, in manual mode it can detect an object before collision and warn to responsible loco pilot so that he/she can control the train manually. In control device there is a toggle switch. If the switch lever goes up then the manual mode will be activated and automatic mode will be activated when the switch lever goes down. There are also two types of light to give signal. High focusable LED light is used for warning. When any object is detected then it will blinking and a green light LED depicts the clearance. There is also a tuner for tuning contrast level of LCD display.

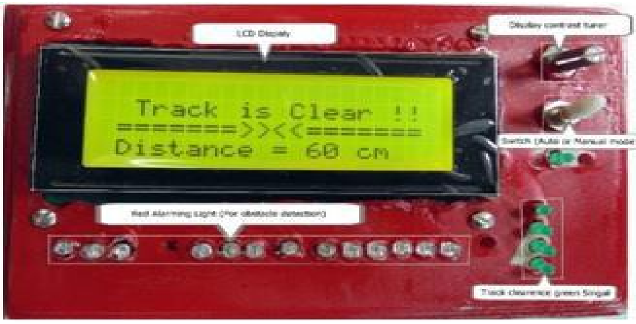

LCD Display
Display contrast tuner
Track is Clear !!
=======>><<=======
Distance = 60 cm
Switch (Auto or Manual mode)
Red Alarming Light (For obstacle detection)
Track clearence green Singal

Fig-5: Our designed control device (Front side).

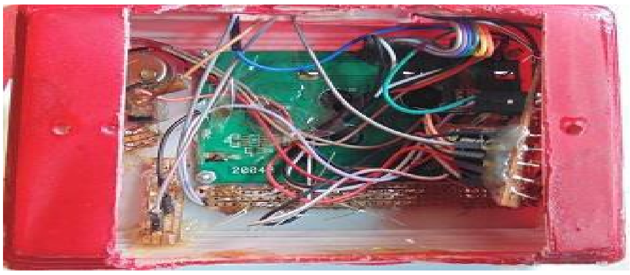


Fig-6: Our designed control device (Back side).

5. RESULT

This experiment comprehends that, it is one of the efficient and dynamic systems for collision object detection and anti-collision system. This technology is based on ultrasonic sound and an embedded system. It has been implemented both in hardware and software module which is capable of preventing any collision between objects and the train when it is in automatic mode at a specific distance. In this experiment we have used a round track and an engine of a toy train where we have included our system. After placing the train on the track, it moves freely in absence of any barrier on the track. Next, a barrier is placed on the track. Since the train detects the obstacle using our system, it gradually slows down the speed by initiating the air brake and finally stops before the collision takes place. Green and red LED signals indicate presence of no obstacle or obstacle respectively. Our experiment is shown in Fig-6 and Fig-7.

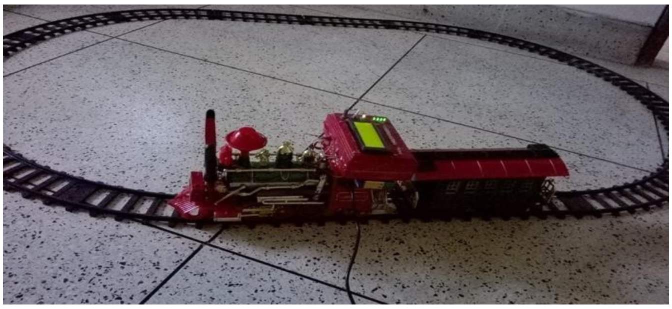


Fig-7: Experimental**.** No barrier is on the track.

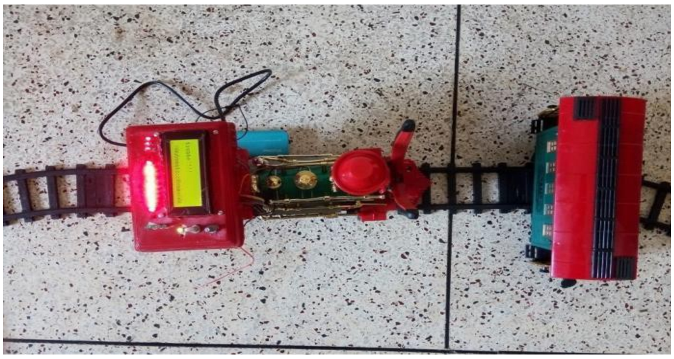


Fig-8: Experimental**.** A barrier is placed on the track.

In Fig-7 there is no obstacle on the track, therefore the train moves freely. On the other hand, in Fig-8 the train stops after observing an obstacle on the track.

6. CONCLUSION

In this paper, we have designed and implemented an innovative technology for collision objects detection and avoiding technique that can prevent any kind of collision with train efficiently. We are confident that incorporating our Anti Collision System with Railway system, it is possible to improve the safety of Railway.

REFERENCES

[1] P. Kiran Kumar, B.S. ShivaShankara ,"PLC Based Automatic Fault Detection of Railway Track and Accidence Avoidance system", International Journal of Engineering Research and General Science,Volume 3, Issue 2, March-April, 2015

[2] Mr. N. Sambamurthy, Sk. Hasane Ahammad,"Prevention of Train Accidents Using Wireless Sensor Networks",Int.Journal of Engineering Research and Applications, Vol. 3, Issue 6, Nov-Dec 2013.

[3] T. Saijyothsna, P. Umamaheswari,"Collision Avoidance of Trains by Creating Mutual Communication Using Embedded System",International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 7, July 2014.

Implementing Digital FIR Filter (Using Various Windows) on DSP Processor

Mr. R. Radhakrishnan
Assistant Professor,
Department of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Mr. S. Balabasker
Associate Professor,
Department of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Abstract.* This Work focuses on design and implementation of Digital FIR Filters using Window method. For this various windows like Rectangular, Hamming, Hanning, Blackman, Kaiser Windows are used. Then the comparison of the features of these windows is done after implementing these filters on DSP Processor TMS320C50 of Texas Instruments. The advantages of Digital filters over the analog filters are like truly linear phase response, specifications of digital filters does not vary with environmental changes, the frequency response of digital filters can be automatically adjusted if it is implemented using a programmable processor, several input signals or channels can be filtered by one Digital filter without the need to replicate the hardware, filtered and unfiltered data can be saved for further use, performance of digital filters is repeatable, and they can be used at very low frequencies found in many applications where the use of analog filters is impractical. Also digital filters can be made to work over a wide range of frequencies by a mere change of the sampling frequency. Study involves Basics of Digital Filters discussed in Literature review. Architecture of TMS320C50 is discussed & MATLAB program is developed for calculating the filter coefficients. These are used in the assembly language program, which is implemented on TMS320C50 DSP Processor. Finally the comparison of features of above said windows is made based upon the obtained results. In future scope of the work, the adaptive filtering and its advantages are discussed. Also the finite word length effects and their remedies on FIR filter performance are discussed.

1. INTRODUCTION

Filters are characterized as one of the most effective signal processing devices. Digital filters operate in discrete domain to attain the objective of filtering. Traditionally, most digital filter applications were limited to audio and high-end image processing. With advances in process technologies and DSP methodologies the implementation of digital filters is cost-effective. They have drawn attention of many researchers from the last few decades due to their enormous applications in engineering. In control engineering, digital filters are used for system stabilization, identification and modeling [1,2]. These Digital filters not only enriches the biomedical signals such as ECG, EEG, and MRI images but are also used in high-tech lifesaving machinery which are highly useful in medical industry [3–6]. In signal processing, many applications includes removal of noise/ interference, shaping of the signal spectrum [7] and many more. Lots of applications are encountered in the field of telecommunication with improved quality and economy of service provided by digital systems applications [8]. Design of an optimal filter is an important constraint of minimization problem wherein an ideal frequency response is approximated by a finite number of continuous functions. This approximation is computed in terms of difference between the two functions and the design problem is reduced to the minimization of this error. Based on this, there are different established and practiced techniques which are LS method, equi-ripple design method, windowing technique and maximally flat method that exist for the design of FIR filters [9]. A relatively new technique for the FIR filter design problem, specifically based on the L1-norm approximation of the error function was devised in [10]. In this, a mathematical optimization problem was formulated for the minimization of L1-error such that it can be solved using linear programming. This resulted in overcoming the problem of non-differentiability and obtaining the unique solution while using L1-approximation in the field of filter design. Also, the FIR filter response in [11] designed with L1-approximation and employing a modified Newton's algorithm for the optimal solution yields a flat pass band as well as stop band in comparison with other techniques. This algorithm exploits the differentiability of the L1-norm and calculates the optimal filter based on the mathematical theory of L1 filters in [12]. All these classical methods are complex and require loads of computations. Some major drawbacks associated with these techniques are summarized. (i) For solving the multi-modal optimization problem such as the designing of FIR filter, a continuous and differentiable objective function is required. (ii) With the increase in number of solution parameters, the search space is increased which reduces the searching capability of the algorithms. As a result, they are highly sensitive to initial bounds. (iii) They are unsuitable for optimizing non uniform, nonlinear, non-differentiable and multi-dimensional fitness function, and hence usually diverge to some local optimal solution [13]. (iv) These algorithms demand a number of runs to obtain an optimized solution and therefore, require a better control of parameters for fast and global convergence. (v) Their computational cost increases with the slow convergence rate and demands a handful experience for the tuning of parameters. To overcome the shortcomings of classical methods, different nature-inspired algorithms got evolved. In recent years, researchers have analyzed that the optimization algorithms designed by modeling the natural procedures are advantageous in solving numerical optimization problem in many science and engineering domains.

2.MATERIAL & METHODS

FIR filters can be designed using various techniques. The most popular Window method is used for designing a FIR filter. FIR Filter is implemented using TMS320C50 Processor. Finally based upon the response of that filter, the response characteristics of filters based on various Windows like Rectangular, Hanning, Hamming and Blackman are compared.

2.1 ALGORITHMS USED

2.1.1 For filter coefficient calculation using MATLAB:

(i) Specify the Sampling Frequency and calculate the Nyquist frequency.
(ii) Specify the Pass band edge and Stop band edge frequencies. Calculate the Normalized Cutoff Frequency. Then calculate the Order of the filter.
(iii) Specify the Window function and calculate the Window coefficients. Then find rounded off filter coefficients in Q-15 format. (x 2^{15})
4.Convert them into Hexadecimal Equivalent and generate output in a text file, so that they can Be fired into the Program Memory of the DSP Processor

2.1.2Assembly Program For implementation of FIR filter on TMS320C50 DSP Processor:

(i) Move filter coefficients from Program memory to Data memory.
(ii) Take Input sample from ADC input port and store at appropriate memory location.
(iii) Set a counter based on the order of the filter N. Also clear accumulator to store the result.
(iv)Perform the linear Convolution between input samples x(n) (New sample & N-1 past samples) and N filter coefficients h(n) to generate output samples y(n).
(v)Move the output sample at the DAC output port.
(vi)Repeat from step 2.

2.2 WINDOW METHOD FUNCTIONS SUPPORTED IN MATLAB.

2.2.1 Rectangular window MATLAB Syntax w=**boxcar (**n)
w = **boxcar** (n,'*sfla++g*')

Description
w = boxcar (n) returns the n-point symmetric Rectangular window in the column vector w, where n is a positive integer.

w = boxcar (n,'*sflag*') returns an n-point Rectangular window using the window sampling specified by '*sflag*', which can be either 'periodic' or 'symmetric' (the default). When 'periodic' is specified, Rectangular computes a length n+1 window and returns the first n points.

2.2.2 Blackman window

MATLAB Syntax w = **blackman**(n)

w = **blackman**(n,'*sflag*')
Description
w = blackman(n) returns the n-point symmetric Blackman window in the column vector w, where n is a positive integer.

w = blackman(n,'*sflag*') returns an n-point Blackman window using the window sampling specified by '*sflag*', which can be either 'periodic' or 'symmetric' (the default). When 'periodic' is specified, blackman computes a length n+1 window and returns the first n points.

The equation for computing the coefficients of a Blackman window is

$$w[k+1] = 0.42 - 0.5\cos\left(2\pi\frac{k}{n-1}\right) + 0.08\cos\left(4\pi\frac{k}{n-1}\right), \quad k = 0, \ldots, n-1$$

Blackman windows have slightly wider central lobes and less sideband leakage than equivalent length Hamming and Hann windows.

2.2.3 Hamming window

MATLAB Syntax w = **hamming**(n)
w= **hamming**(n,'*sflag*') Description

w = hamming (n) returns an n-point symmetric Hamming window in the column vector w. n should be a positive integer.
The coefficients of a Hamming window are computed from the following equation.

$$w[k+1] = 0.54 - 0.46\cos\left(2\pi\frac{k}{n-1}\right), \qquad k = 0, \ldots, n-1$$

w = hamming(n,'*sflag*') returns an n-point Hamming window using the window sampling specified by '*sflag*', which can be either 'periodic' or 'symmetric' (the default). When 'periodic' is specified, hamming computes a length n+1 window and returns the first n points.

2.2.4 Hanning window

MATLAB Syntax w = **hann**(n)
w= **hann**(n,'*sflag*')

Description

w = hann(n) returns an n-point symmetric Hann window in the column vector w. n must be a positive integer. The coefficients of a Hann window are computed from the following equation.

$$w[k+1] = 0.5\left(1-\cos\left(2\pi\frac{k}{n-1}\right)\right), \qquad k = 0, \ldots, n-1$$

w = hann(n,'*sflag*') returns an n-point Hann window using the window sampling specified by '*sflag*', which can be either 'periodic' or 'symmetric' (the default). When 'periodic' is specified, hann computes a length n+1 window and returns the first n points.

3.SYSTEM & IMPLEMENTATION

The 'C5x uses an advanced, modified Harvard-type architecture based on the 'C25 architecture and maximizes processing power with separate buses for program memory and data memory. The instruction set supports data transfers between the two memory spaces. The 'C5x architecture is built around four major buses:

Program bus (PB)
Program address bus (PAB)
Data read bus (DB)
Data read address bus (DAB)

The PAB provides addresses to program memory space for both reads and writes. The PB also carries the instruction code and immediate operands from program memory space to the CPU. The DB interconnects various elements of the CPU to data memory space. The program and data buses can work together to transfer data from on-chip data memory and internal or external program memory to the multiplier for single-cycle multiply/accumulate operations. The 'C5x has 96 registers mapped into page 0 of the data memory space. All 'C5x DSPs have 28 CPU registers and 16 input/output (I/O) port registers but have different numbers of peripheral and reserved registers. Since the memory-mapped registers are a component of the data memory space, they can be written to and read from in the same way as any other data memory location. The memory-mapped registers are used for indirect data address pointers, temporary storage, CPU status and control, or integer arithmetic processing through the ARAU.

4.RESULTS & DISCUSSION

By analysing the generated outputs, the inferences are made about the important features of the FIR filters based
upon various Windows. Each Window has special characteristics like main lobe width, maximum side lobe magnitude and effect of frequency on side lobe magnitude. Any window can be selected for the design of FIR filter, depending upon the desirable characteristics of that window.

Fig 4.1 shows the Rectangular window The width of main lobe in window spectrum is 4/N.The maximum side lobe magnitude in window spectrum is –13dB. In window spectrum the side lobe magnitude slightly decreases with increasing . In FIR filter design using rectangular window the minimum stop band attenuation is 22dB

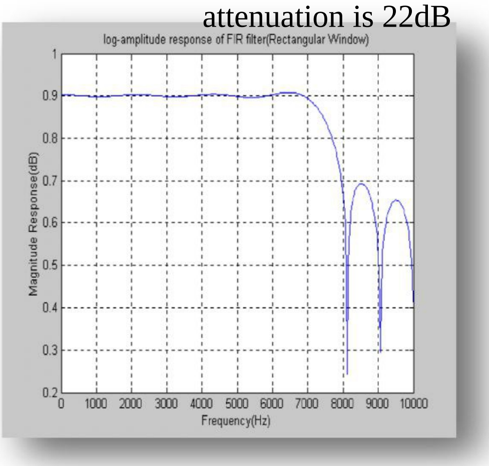


Figure 4.1 Log Amplitude Response of Rectangular Window

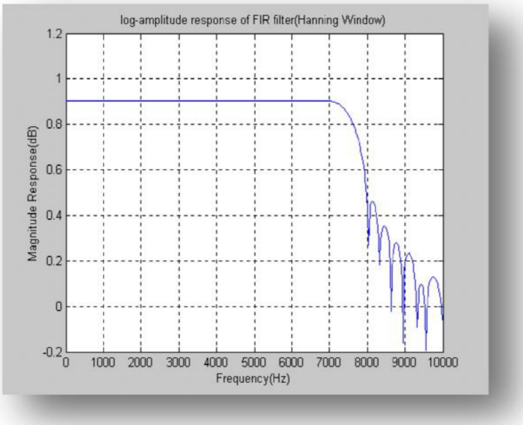


Figure 4.2 Log Amplitude Response of Hanning Window

Fig 4.2 shows Hanning The width of main lobe in window spectrum is 8/N. The maximum side lobe magnitude in window spectrum is –31dB. In window spectrum, the side lobe magnitude decreases with increasing . Using Hanning window, the minimum stop band attenuation is 44dB.

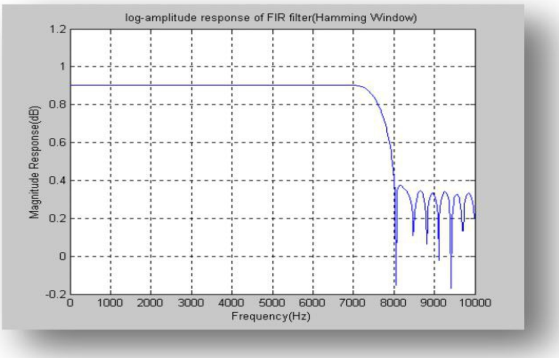


Fig 4.3 Log Amplitude Response of Hamming Window

The width of main lobe in window spectrum is 8□/N. The maximum side lobe magnitude in window spectrum is – 41dB.In window spectrum, the side lobe magnitude remains constant. In FIR filter design using Hamming window, the minimum stop band attenuation is 51dB

5.CONCLUSION

There are four ways in which these performance of FIR filter is improved:

a) ADC Noise: caused by limited no. of bits to be used for ADC output, which results in lower S/N ratio. The error due to this can be avoided by using additional bits for ADC output

b) Coefficient Quantization errors: this result from representing filter coefficients with a limited no of bits. This can be solved using enough bits to represent filter coefficients. Different optimization techniques can be used for efficient selection of the coefficients to minimise these errors.

c) Round off Errors from Quantizing results of arithmetic operations: These occur when the lower order bits are discarded before storing the results of multiplications. This is normally forced due to word length limitations of the processors used.Rounding after double length summing of products may reduce the error due to this effect.

d)Arithmetic Overflow: This occurs when partial sums or filter output exceeds the word length of the processor. This results in wrong output samples (normally the sign changes). To avoid this overflow the filter coefficients can be scaled by dividing each filter coefficient by a factor such that the output sample never exceeds the permissible world length.

REFERENCES

[1] Panda G, Pradhan PM, Majhi B. IIR system identification using cat swarm optimization. Expert Syst Appl 2011;38: 12671–83.

[2] Alera R, Vegab A, Galvana IM, Nebroc AJ. Multi-objective metaheuristics for preprocessing EEG data in braincomputer interfaces. J Eng Optimiz 2012;44(3):373–90.

[3] Karthik GVS, Fathima SY, Rahman MZU, Ahamed SR, LayEkuakille A. Efficient signal conditioning techniques for brain activity in remote health monitoring network. IEEE Sens J 2013;13(9):3276–83.

[4] Rawat TK. Digital signal processing. 1st ed. Oxford University Press; 2014.

[5] Saha SK, Kar R, Mandal D, Ghoshal SP. Bacteria foraging optimisation algorithm for optimal FIR filter design. Int J BioInspired Comput 2013;5(1):52–66.

[6] Rashedi E, Hossien N, Saryazdi S. Filter modelling using gravitational search algorithm. Eng Appl Artif Intell 2011;24 (1):117–22.

[7] Kumar M, Rawat TK. Optimal design of FIR fractional order differentiator using cuckoo search algorithm. Expert Syst Appl 2015; 42:3433–49.

A Survey on Smart Home Based Systems Using Wi-Fi

[1]Mrs.C.Suganya, [2]Ms.S.K.Suriya, [3]Ms.S.Devika
[1,2,3] Assistant Professor,
Department of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

ABSTRACT: Current WiFi systems support a peak physical-layer data rate of 54 Mbps and typically provide indoor coverage over a distance of 100 feet. Conventional sensing methodologies for smart home are known to be labour-intensive and complicated for practical deployment. Thus, researchers are resorting to alternative sensing mechanisms. WiFi is one of the key technologies that enable connectivity for smart home services. Apart from its primary use for communication, WiFi signal has now been widely leveraged for various sensing tasks, such as gesture recognition and fall detection, due to its sensitivity to environmental dynamics. Building smart home based on WiFi sensing is cost-effective, non-invasive, and enjoys convenient deployment. In this paper, we survey the recent advances in smart home systems based on WiFi sensing, mainly in such areas as health monitoring, gesture recognition, contextual information acquisition, and authentication.

Key words: IoT, Smart home, WiFi sensing

I INTRODUCTION

Smart home technology, also known as home automation, provides homeowners security, comfort, convenience and energy efficiency by allowing them to control smart devices, often by a smart home app on their smart phone or other networked device. A part of the internet of things (IoT), smart home systems and devices often operate together, sharing consumer usage data among themselves and automating actions based on the home owners preferences. Smart home enables the interconnections of ubiquitous devices planted in home appliance with sensors and actuators for automation. The thrust for smart home is an aggregation of different kinds of technologies which normally involve three layers: application layer, network layer, and perception layer.

Recent advances in wireless technology have found that the WiFi signals are sensitive enough to capture environmental dynamics thus can be used for the sensing purpose. Building a smart home based on WiFi sensing can outweigh conventional solutions. The main benefits are threefold. 1) Cost effective. WiFi sensing makes it possible to deploy sensing tasks on existing infrastructures, namely WiFi transceivers which are already ubiquitous in typical indoor settings. 2) Convenient deployment. Building supported hardware for smart home is simple and easy.

II WIFI SENSING

WiFi sensing is an emerging concept that uses WiFi radios as sensors. We introduce two numerical "sensor" readings, namely Received Signal Strength Indicator (RSSI) and Channel State Information (CSI). Received Signal Strength Indicator (RSSI) defines the relative power strength of the received signal. In IEEE 802.11 standard, RSSI is internally used to reflect a link quality [36]. RSSI follows the Log-normal Distance Path Loss (LDPL) model.

$$P(d) = P(d_0) + 10nlg(\frac{d}{d_0}) + X_\delta$$

Where,

P(d) is the power strength at distance d
P(d0) denotes the power strength at a reference location d0
n is the power loss coefficient
Xδ is a random noise

Channel State Information (CSI) is a much finer grain metric than RSSI. CSI has been widely adopted in wireless communication especially in modern Orthogonal Frequency Division Multiplexing (OFDM) systems. The primary function of CSI is to estimate the properties of propagation channel characterized by the environment dynamics, thus adopting better strategies to improve throughput performance.

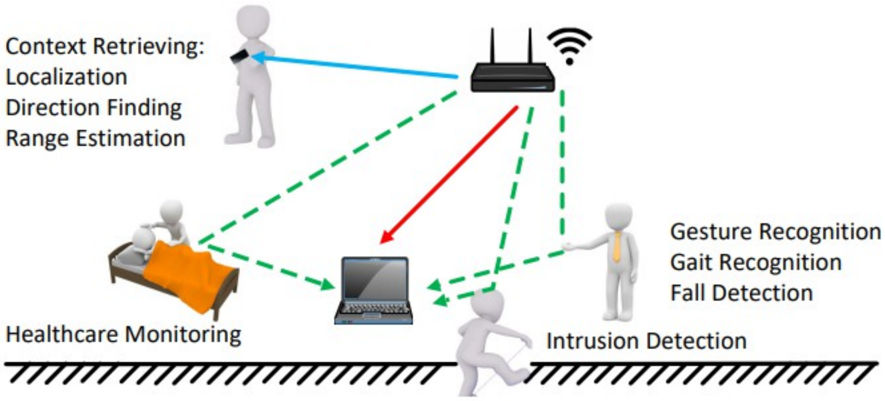


Fig. 1. Overview of application based on wifi sensing

III APPLICATIONS BASED ON WIFI SENSING

WiFi sensing, which can be divided into four categories: health monitoring, gesture recognition, contextual information acquisition, and authentication. The physical layer configurations for these applications normally involve one pair or several pairs of WiFi-enabled transceivers to be deployed in different places. The processing layer for these applications can be generalized into model-based or learning method based. Some works may combine the two models together. Model-based methods build the systems in a divide-andconquer manner, consisting of a pipeline of signal processing blocks. Instead of explicitly finding a perfect model, some researchers resort to machine learning techniques. Machine learning based methods typically involve two steps: the offline training and the online predicting. The offline training step is supposed to produce a model, which correlates certain events to the specific features of WiFi signal. When the system is online, the WiFi signal, after some pre-processing procedures, namely de-noising and feature extraction, will be fed into the model to predict certain events.

IV HEALTH MONITORING WITH WIFI SENSING

Currently, most of the health monitoring systems depends on dedicated devices. Many are limited to clinic use and require a well-trained technician to set up. Even though there are some portable devices developed for household use, they are still far from user-friendly and require specialists to instrument the sensors. To make matters worse, some medical disorders, such as sleep apnea, when breathing becomes abnormal during sleep, need constant monitoring. In the clinic, doctors often use polysomnography test to diagnose sleep apnea, which is expensive and laborious. So a non-invasive method is more desirable. Health monitoring systems with WiFi sensing are promising alternatives to overcome the above limitations. By leveraging the invisible WiFi radios, the sensing tasks can be completed without user awareness, which causes minimum discomfort. The WiFi radios can traverse through walls, making it feasible to perform sensing tasks even under challenging NLOS scenarios. The multipath effect, which is normally detrimental for data communication, can have a beneficial effect on WiFi sensing as it extends the spatial sensing dimensions. We now introduce WiFi-enabled systems capable of detecting biomedical information, for example, respiration rate, heartbeat, and abnormal behaviors. WiFi-enabled fall detection systems [19], [20] harness the fact that a sudden fall can cause abrupt changes in CSI values. To detect the respiration rate or heartbeat is much more difficult, as such activities do not introduce noticeable difference on the numerical sensing results. Hence, such systems often require the transceivers placed near the human body. The rational for respiration rate detection is that the miniature chest displacement can modulate the radio signal.

V WIFI-ENABLED GESTURE RECOGNITION

Gestures refer to expressive and meaningful body motions including physical movements of different body parts such as fingers, hands, arms, heads, and faces, aiming to interact with the surrounding. Gesture recognition systems aim to recognize conveyed messages behind performed gestures. Applications of gesture recognition range from recognizing sign language through home automation to virtual reality. It is the key enabler for designing a highly efficient and intelligent Human Computer Interface (HCI). Two well-known commercial gesture recognition systems are Xbox Kinect which is based on vision technology and Wii , a wearable device based on the Inertial Measurement Unit (IMU). Vision technology requires the camera directly "see" the gesture performers with a good light condition. And some people may be unwilling to wear specific devices. Wifi-enabled gesture recognition can largely overcome the above limitations since it can achieve devicefree. Most of the WiFi-based gesture recognition applications adopt machine learning techniques for pattern recognition.

VI. CONCLUSION

In this paper, we surveyed state-of-the-art smart home systems and applications based on WiFi sensing. We discussed the principles, capabilities, and limitations of these works. Overall, WiFi sensing is a promising technology for a broad spectrum of smart home applications, which however has yet to be a perfect replacement for conventional sensing mechanism due to various practical concerns. The recent advances in deep learning may offer great help for developing configuration-free systems.

REFERENCES

[1] P. Sethi and S. R. Sarangi, “Internet of things: Architectures, protocols, and applications,” Journal of Electrical and Computer Engineering, vol. 2017, pp. 1–25, Jan 2017.
[2] S. Kraijak and P. Tuwanut, “A survey on iot architectures, protocols, applications, security, privacy, real-world implementation and future trends,” in 11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015), 2015.
[3] Q. Guan, C. Li, X. Guo, and B. Shen, “Infrared signal based elderly fall detection for in-home monitoring,” in 2017 9th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC), 2017.
[4] L. Minvielle, M. Atiq, R. Serra, M. Mougeot, and N. Vayatis, “Fall detection using smart floor sensor and supervised learning,” in 2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), 2017.
[5] A. Virmani and M. Shahzad, “Position and orientation agnostic gesture recognition using wifi,” in Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys), 2017.
[6] W. Wang, A. X. Liu, M. Shahzad, K. Ling, and S. Lu, “Understanding and modeling of wifi signal based human activity recognition,” in Proceedings of the 21st Annual International Conference on Mobile Computing and Networking (MobiCom), 2015.
[7] D. Halperin, W. Hu, A. Sheth, and D. Wetherall, “Tool release: Gathering 802.11n traces with channel state information,” SIGCOMM Comput. Commun. Rev., vol. 41, no. 1, pp. 53–53, Jan. 2011.
[8] Y. Xie, Z. Li, and M. Li, “Precise power delay profiling with commodity wifi,” in Proceedings of the 21st Annual International Conference on Mobile Computing and Networking (MobiCom), 2015.
[9] Y. Wang, J. Liu, Y. Chen, M. Gruteser, J. Yang, and H. Liu, “E-eyes: Device-free location-oriented activity identification using fine-grained wifi signatures,” in Proceedings of the 20th Annual International Conference on Mobile Computing and Networking (MobiCom), 2014.

Multi-Role Unmanned Ground Vehicle for Rescue and Defense Applications

[1]Ms.M.Keerthana, [2]Ms.A.Nilofarnisha
[1,2] UG Scholar,
Department of Electronics and Communication Engineering,
V.R.S. College of Engineering and Technology,
Arasur-607017, Tamil Nadu.

Mr.V.Thiyagarajan
Associate Professor,
Department of Electronics and Communication Engineering,
V.R.S. College of Engineering and Technology,
Arasur-607017, Tamil Nadu.

Abstract - Nowadays the world is very insecure due to various problems like terrorism, natural disasters, emergency health situations and surveillance. Valuable lives are being lost in various situations due to human negligence when carrying out rescue or emergency operations. Even though when our security forces are tireless working to save us every day, we still have problem to entirely secure ourselves in different situations. To counter these issues we propose a project. Our project is a multi-role capable unmanned ground vehicle. The current types of unmanned ground vehicles are designed for doing only one specific task like bomb detection, live human detection, border alert system, assisting robot etc., but our unmanned ground vehicle is designed to undertake multiple tasks. The robot is equipped with a PIR sensor to detect live human, metal detector for bomb detection, detect the obstacle by capturing the border alert using camera. Raspberry Pi 2 is used to control the Unmanned Ground Vehicle (UGV) and is the core of UGV and DC motors attached to perform forward and reverse movements. This UGV can detect live human and bomb detection, monitor condition of the place like temperature and presence of natural gas. A camera is attached with this UGV with which it can observe the condition of the border system. It also contains a coil gun with which it can attack enemy within a range of 10 fit and has also obstacle detector to protect itself. By implementing a mix of modular design, simple and cheap circuitry we can develop an effective and reliable multi- role capable unmanned ground vehicles.

Keywords: Raspberry Pi, Python, PIR Sensor, Open CV, Surveillance.

I. INTRODUCTION

An unmanned ground vehicle (UGV) is being developed day by day in different applications like military and civilian operations, surveillance, border patrolling, law enforcement, hostage situation, and police for some specific mission to detecting and diffusing bombs. A timely rescue can only save the people who are buried and wounded due to a disaster. In such situations, rescue system must take fast decisions under pressure, and try to get victims to safe location at their own risk. The rescue system must collect the location information and status of victims as quickly as possible so that medication and fire-fighters can enter the disaster prone area and save people. All these works are performed mostly in very dangerous and risky situations by human and trained dogs. Detection by rescue workers becomes time consuming and due to the vast area that gets affected it becomes more difficult. So the project proposes a rescue robot that moves in a disastrous area and helps in identifying the live people and rescue operations. We are introducing an UGV which senses the movement in border area without manpower and launches its gun towards the target. A unique Passive Infrared sensor is used in the project which emits infrared rays to detect humans. As live human body emits thermal radiation it is received and manipulated by the PIR sensor to detect humans. The real time bomb sensor is not used because of the variable composition of bomb material, a metal sensor or magnetic sensor can be used as a proto-type and can be replaced by a real bomb sensor if used practically widely for the purpose.

II. PROPOSED SYSTEM

The objective of this project is to implement automation of unmanned ground vehicle with the help of raspberry pi 2B. The project proposes a multi-role unmanned ground vehicle that moves in the battle field and helps in identifying the live people those are injured and performs rescue system operations and monitoring border alert system. There is a communication link between control unit and UGV unit via Zig-Bee Link. One raspberry pi 2B model, a wireless camera, array of sensors, motor driver circuitry to control and drive the motors and Zig-Bee modem Circuitry to transmit and receive signal being send by UGV unit. Then the sensors (PIR, Gas, Metal, Obstacle), motors, coil gun were connected according to the design. Here the Zig-Bee module used for receiving the transmitted signal from the transmitter.

Outputs of sensors are connected to Raspberry Pi processor shown in figure 1 then outputs are processed and according to sensors' outputs functions are performed. Also information is transmitted to control room unit shown in figure 2 via ZigBee transceiver for monitoring purpose. Images are captured by wireless camera which is used to detect enemies crossing border. Based on that coil gun is targeting enemy and hit him as well as images are transmitted to control room unit for defense applications.

2.1 Unmanned Ground Vehicle

The vehicle can be operated autonomously i.e (able to work without human). It is widely used where inconvenient, hazardous or difficult to handle the situation by human operators. It has the ability to track the path, gather user about the environment, period of working can be extended without the help of operators. They can also repair themselves without outside assistance. They can be widely used in Defense applications, Agriculture, Industries, etc,. It can able to monitor and self-restrained machine.

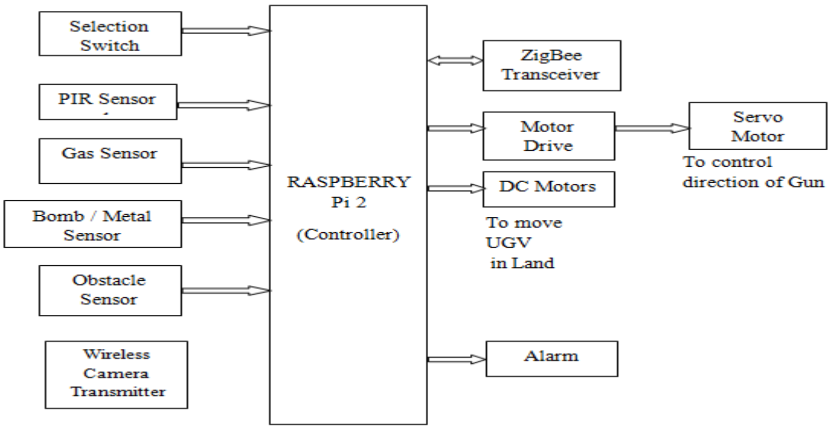


Figure 1: Block diagram of Proposed Unmanned Ground Vehicle

2.2 Control Unit

The control unit compromises of a PC, GUI interface software, a Zig-Bee Rx-Tx duplex communication modem, a level converter which converts host computer control signal to Zig-Bee compatible signal and a driver interface card. A wireless RF receiver is used to receive the footages send by the camera placed on the UGV unit to visualize the live video of the place where the UGV is present. Using a driver interface card, the can be seen on the host PC or can be directly seen on a television without using any interface card. Though the PC does not understand the signal received by Zig-Bee, we use Level-Converter in between PC and modem to change the level of signal and make the signal PC acceptable.

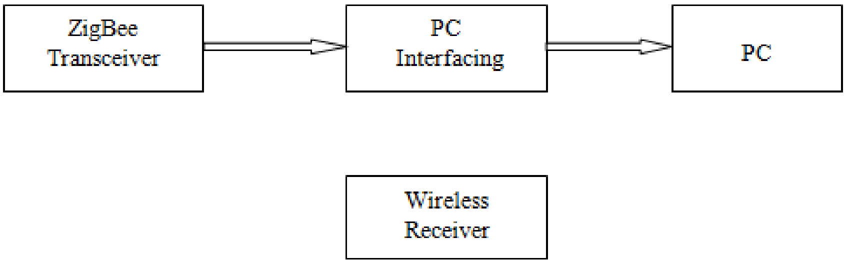


Figure 2: Control Room Unit

III.HARDWARE & SOFTWARE IMPLEMENTATIONS

3.1 Hardware Requirements:

Raspberry Pi 2B
ZigBee Transceiver
Wireless Camera
Servo Motor
DC Motor
PIR Sensor
GAS Sensor
Metal Sensor
Obstacle Sensor
Buzzer

3.2 Software Requirements:

Python Language
Raspbian OS

3.3 Raspberry Pi 2:

The raspberry pi 2 is core kit which replaces the personal computer and does the process very efficiently. The method includes vital hardware components and software. It is a small sized single board computer. The Raspbian OS installed in the Raspberry pi 2B kit and the necessary library functions are installed using python libraries.

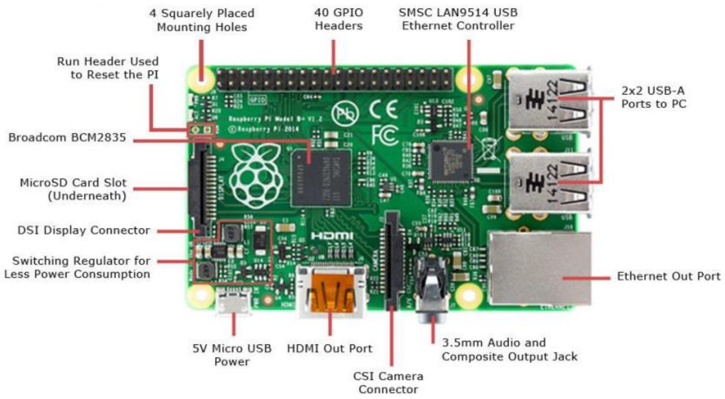

4 Squarely Placed Mounting Holes
40 GPIO Headers
SMSC LAN9514 USB Ethernet Controller
Run Header Used to Reset the PI
2x2 USB-A Ports to PC
Broadcom BCM2835
MicroSD Card Slot (Underneath)
DSI Display Connector
Switching Regulator for Less Power Consumption
Ethernet Out Port
5V Micro USB Power
HDMI Out Port
CSI Camera Connector
3.5mm Audio and Composite Output Jack

Figure 3: Overview of the Raspberry Pi 2.0 B

3.4 Raspbian OS - Noobs:

Among all operating system such as Risc OS, Chromium OS, Angstorm Linux, Pidora, Gentoo, Raspbian is the best one for Raspberry. It is feasible for working and also free operating system available in the website. Raspbian also has types as wheezy, Jessie, noobs. We prefer noobs because it improves the performance and flexibility, particularly as regards the control of the system processes, fast, pre-programmed, high capacity and as with any update, there are also numerous bug fixes and tweaks.

3.5 Python:

It is high level programming language which allows coders to express their ideas in fewer lines when compared other programming languages like C, C++, Java. It also had large number of packages and also used to combine software with hardware. Python can be executed directly by the system without compiling it. So the execution time is very less when compare with other programming languages.

3.6 ZigBee Transceiver:

It is used to send and receive data between UGV and the control unit. Zigbee is a digital wireless communication protocol. It is a very low power communication technology. Zigbee is a very versatile communication technology. XBee and XBee-PRO Modules were engineered to meet Zigbee/IEEE 802.15.4 standards and support the unique needs of lowcost, low-power wireless sensor networks. The modules operate within the ISM 2.4 GHz frequency band and are pin-for-pin compatible with each other.

3.7 Power Supply Unit:

In this circuit, the required power is 5V for micro-controller and motor driver IC, 3.3V for Zig-Bee and 6V for motors. Thus, the Power supply is given to the circuit by 230V AC for Control unit and via 6V battery in UGV unit. The L293D motor driver IC is designed to provide a bidirectional drive currents of up to 600mA at voltages from 4.5 V to 36 V. Devices are designed to drive inductive loads such as relays, dc and bipolar stepping motors.

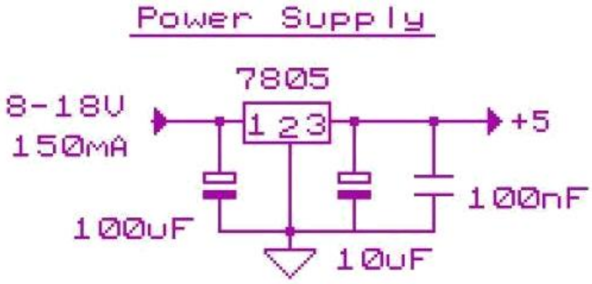


Figure 4: Regulated DC Power Supply

3.8 DC Motor:

DC Motors can rotate in two directions depending on polarity of the battery connected to the motor. Both the DC motor and the battery are two terminal devices that have positive and negative terminals. In order run the motor in the forward direction, connect the positive motor wire to the positive battery wire and negative to negative. However, to run the motor in reverse just switch the connections; connect the positive battery wire to the negative motor wire, and the negative battery wire to the positive motor wire. An H-Bridge circuit allows a large DC motor to be run in both directions with a low level logic input signal. Here we use four DC motors for moving UGV.

3.9 Servo Motor:

A servomotor is a rotary actuator or linear actuator that allows for precise control of angular or linear position, velocity and acceleration. It consists of a suitable motor coupled to a sensor for position feedback. It also requires a relatively sophisticated controller, often a dedicated module designed specifically for use with servomotors. Servos are controlled by sending an electrical pulse of variable width, or pulse width modulation (PWM), through the control wire. There is a minimum pulse, a maximum pulse, and a repetition rate. Servo motors can usually only turn 90 degrees in either direction for a total of 180 degree movement. The motor's neutral position is defined as the position where the servo has the same amount of potential rotation in the both the clockwise or counter-clockwise direction. This motor is used to target the coil gun.

3.10 Wireless Camera:

To visualize the live environment around the robot, a wireless mini RF camera is used. There are two units of Camera, receiving unit and transmitting unit. Transmitting unit contains of camera with a RF transmitter and Receiving unit compromises with an RF antenna and a signal processing driver unit. In addition to that if we use PC to watch the footages, an additional Driver Interface Card will come into the picture to change the signal level to PC compatible.

Figure 5: Wireless Mini Camera

3.11 Sensors used in UGV:

3.11.1 PIR Sensor:

As live human body emits thermal radiation it is received and manipulated by the PIR sensor to detect humans. PIR sensors are passive infrared sensors. They detect change in the heat and this can be used to detect movement of people. It has digital output and can be directly given to Integrated Intelligent Research (IIR) the digital pins and no ADC is needed. It operates at 5V DC. The PIR (Passive Infra-Red) Sensor is a pyroelectric device that detects motion by measuring changes in the infrared (heat) levels emitted by surrounding objects. This motion can be detected by checking for a sudden change in the surrounding IR patterns. When motion is detected the PIR sensor outputs a high signal on its output pin. This logic signal can be read by a microcontroller or used to drive a transistor to switch a higher current load. Detection ranges up to 20 feet away.

Figure 6: PIR Sensor

3.11.2 METAL Sensor:

A Bomb/Metal sensor detects the presence of suspected material in Rescue operation. The real time bomb sensor is not used because of the variable composition of bomb material, a metal sensor or magnetic sensor can be used as a proto-type and can be replaced by a real bomb sensor if used practically widely for the purpose.

3.11.3 GAS Sensor:

MQ05 gas sensor has been used in the UGV. It will sense if there is any unusual gas present or not. If detects any gas, it will send the data to the microcontroller.

3.11.4 Obstacle Detector:

An obstacle detector sensor implemented to the UGV to prevent any damage to the body of the UGV as well finding border line. If it found any obstacle very near to the body of the UGV, it will prevent the forward movement of the UGV.

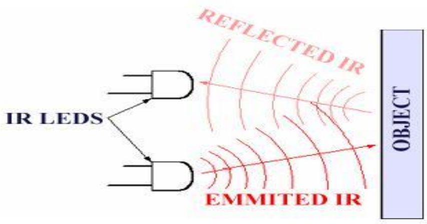


Figure 7: Object Detection Using IR Light

3.12 Coil Gun:

The coil gun contains two parts.

Charge Control Part:

To shoot through the coil gun high voltage need to boost the coil. To supply high energy two 400v 220µF capacitor has been used. To charge the capacitor a high frequency inverter has been used.

Coil:

To shoot through the coil gun an electro magnet need to produce. 20ft long insulated wire used to make the coil to produce the elector magnet. Coil gun able to shoot any object within the range of 10 feet.

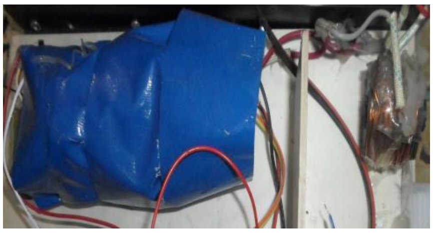


Figure 8: Coil Gun Circuit

3.13 Buzzer:

This buzzer is an electromagnetic type audio signaling device, which has a coil inside which oscillates a metal plate against another, which when given voltage difference produces sound of a predefined frequency. You must be aware of such sounds of buzzer like BEEP sound in many appliances.

Figure 9: Buzzer

IV. APPLICATIONS

The application of the use of unmanned ground vehicle are immense some of the real applications of the vehicle are as follows

a. Bomb detection and handling
b. Surveillance
c. Multi-role capacity
d. Border alert system
e. Disaster situations

V. CONCLUSION

This system demonstrates the use of unmanned ground vehicle designed for multi-role capabilities like the robotic arm for metal detector to detect bombs, surveillance, live human detection, border alert system etc. The unmanned system is a game changing technology that everyone is betting the future to be filled with unmanned system. We have already seen a lot of unmanned systems coming into our social lives like the drones, serving food etc., and this is just the beginning of a new revolution our day to day lives. This project sets a example of the current trend of the use of unmanned system in the military defense applications.

REFERENCES

1. A. Mugan, A. bner, A. Apak, C. Dikilita, H. Heceoglu , V. Sezer, Z. Ercan,and M. Gokasan "Conversion of a conventional electric automobile into an unmanned ground vehicle (UGV)", Proceedings of the IEEE International Conference on Mechatronics, 2012.
2. A. Mohebbi, M. Keshmiri,S. Safaee, and S. Mohebbi, "Design, Simulation and manufacturing of a Tracked Surveillance Unmanned Ground Vehicle", Proceedings of the IEEE International Conference on Robotics and Biomimetices, pp.14-18; 2010.
3. Md. Ajijul bin zabbar, Nafiz ahmed chisty " Design & mplementation of an Unmanned Ground Vehicle Surveillance Robot" International Journal of Electrical and Electronics Engineering (IJEEE); 2016.
4. Hardeep Pal Sharma; Guna sekar.C.H "Live Human Detecting Robot for Earthquake Resque Operation", Vol. 2, Issue 01, June 2013.
5. Sivasoundari, S.Kalaimani, M.Balamurugan: "Wireless Surveillance Robot with Motion Detection and Live Video Transmission"," *International Journal of Emerging Science and Engineering (IJESE)"* ISSN: 2319–6378, Volume-I, Issue-6 April 2013.
6. Trupti B. Bhondve, Prof.R.Satyanarayan, Prof. Moresh Mukhedkar: "Mobile Rescue Robot for Human Body Detection in Rescue Operation of Disaster", "*International Journal of Advanced Research in Electrical,Electronics and Instrumentation Engineering"*, Vol. 3, Issue 6, June 2014.
7. Jai rajesh.P, Dhanasekar J, V.G. Vijaya " multi-role unmanned ground vehicle for bomb detection and surveillance" , "*International Journal of Pure and Applied Mathematics"* Volume 116, 2017.
8. An autonomous wireless sensor network deployment system using mobile robots for human existence detection in case of disasters Ad Hoc Networks 13 (2014) 54–68.
9. Alive human body detection system using an autonomous mobile rescue robot India Conference *(INDICON)*, 2011 Annual IEEE.

Fabrication of a Prototype Autonomous Weapon Using Quad copter for Military Application

[1]R.Ranjith,[2] P.Arulkumar,[3]S.Syed Abuthakeer,[4]Magimai Bonifal,
[1,2,3,4] UG Scholar
Department of Electronics and Communication Engineering
St.Anne's College of Engineering and Technology, Anguchettypalayam,
Panruti.

V.Venkatesan,
Assistant Professor
Department of Electronics and Communication Engineering
mailto:vv2620@gmail.com, Mobile - 8939150098
St.Anne's College of Engineering and Technology, Anguchettypalayam,
Panruti.

ABSTRACT

The concept of an Unmanned Aerial Vehicle (UAV) has largely been considered one the most innovative and advantageous military accomplishments within the past decades. UAVs, including multicopter and drones, are currently being used for two major purposes military and commercial use. Considering to commercial use a multicopter is integrated with a wireless camera for remote surveillance. This project is about fabrication of a prototype autonomous weapon using multicopter for military application. A quadcopter is built having symmetrical four arms on which a DC brushless motor with propeller is mounted on every arm. To make this quadcopter autonomous, we will be using Arduino platform to program and apply Proportional Integral Derivative (PID) algorithm to calculate the output values of the motor commands by using input values from transmitter and sensors. Inertial Measurement Unit (IMU) sensor will be giving the values regarding angle and angular velocity of the quadcopter. The quadcopter will also be interfaced with a wireless camera for the hawk view which helps in border security, surveillance, counter insurgency, attack and strike, target identification and designation and communication relay. UAVs are better suited for dull, dirty or dangerous mission .

Keyword: UAV, BLDC, Quad Copter

I. INTRODUCTION

Unmanned Aerial Vehicle (UAV), commonly known as a drones or Unmanned Aircraft System (UAS), or by several othernames, is an aircraft without a human pilot aboard. The flight of UAVs may operate by wireless remote control by a human operator, or fully or intermittently autonomously by an autopilot or onboard processor.Compared to manned aircraft, UAVs are often preferred for missions that human cannot enter. Basically it originated from commercial applications, but recently expanding in military application.

II. BLOCK DIAGRAM

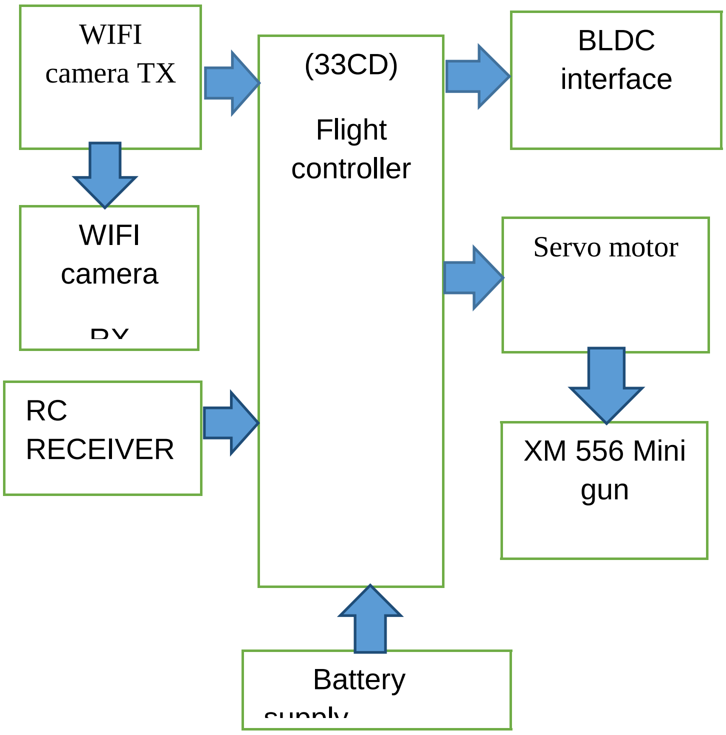


Fig.1 Proposed System Block Diagram

III. WORKING SCENARIO

The aim of this concept is to survey target and take down the enemies through quad copter so that the quad copter can be controlled through the wireless medium. We can survey by using FPV camera so that it transmits live stream of visual information to its FPV camera receiver .The gun is interfaced with quad copter and gun can be controlled by the servo by giving command from the radio transmitter respectively. Whereas all this functions can be controlled by the flight controller

IV. FLIGHT CONTROLLER

Next comes the brain of the quad copter, the flight controller. The flight controller is basically the little computer which controls the craft, and interprets the signals the transceiver sends to guide the quad copter. For builders of quad copter, choosing a flight controller is more of a personal choice in many ways, not unlike choosing from various PC processors in the same power range. Each have various options that each manufacturer wants and may or may not be customizable. If this is something that needs to be fixed, start reading the forums and listen to hobbyists who recommend affordable, reliable controllers which work with most components easily. The flight controller consists ports for interfacing BLCD, radio receiver so that BLDC can obtain variable speed through the ESC and the RC receiver also decodes the encoded information by RC transmitter and feed it to the flight controller to take further actions respectively

V. RADIO TRANSMITTER

The transmitter itself generates a radio frequency alternating current, which is applied to the antenna. When excited by this alternating current, the antenna radiates radio waves. The term transmitter is usually limited to equipment that generates radio waves for communication purposes; or radiolocation, such as radar and navigational transmitters. A transmitter can be a separate piece of electronic equipment, or an electrical circuit within another electronic device. Transmitter and receiver combined in one unit is called a transceiver. The purpose of most transmitters is radio communication of information over a distance. The information is provided to the transmitter in the form of an electronic signal, such as an audio (sound) signal from a microphone, a video (TV) signal from a TV camera, or in wireless networking devices a digital signal from a computer. The transmitter combines the information signal to be carried with the radio frequency signal which generates the radio waves, which is often called the carrier. This process is called modulation. A radio transmitter is an electronic circuit, which transforms electric power from a battery or electrical mains into a radio frequency alternating current, which reverses direction millions to billions of times per second. The energy in such a rapidly reversing current can radiate off a conductor (the antenna) as electromagnetic waves (radio waves).

VI. RADIO RECEIVER

A radio receiver is an electronic circuit that receives its input from an antenna, uses electronic filters to separate a wanted radio signal from all other signals picked up by this antenna, amplifies it to a level suitable for further processing, and finally converts through demodulation and decoding the signal into a form usable for the consumer, such as sound, pictures, digital data, measurement values, navigational positions, etc. The receiver is the receiving end of a communication channel. It receives decoded messages/information from the sender, who first encoded them. Sometimes the receiver is modelled so as to include the decoder. Real-world receivers like radio receivers cannot be expected to receive as much information as predicted by the noisy channel coding theorem.

VII. BLDC

In a brushless DC motor (BLDC), you put the permanent magnets on the rotor and you move the electromagnets to the stator. Then you use a computer (connected to high-power transistors) to charge up the electromagnets as the shaft turns. This system has all sorts of advantages:

- Because a computer controls the motor instead of mechanical brushes, it's more precise. The computer can also factor the speed of the motor into the equation. This makes brushless motors more efficient.
- There is no sparking and much less electrical noise.
- There are no brushes to wear out.
- With the electromagnets on the stator, they are very easy to cool.
- You can have a lot of electromagnets on the stator for more precise control.

The only disadvantage of a brushless motor is its higher initial cost, but you can often recover that cost through the greater efficiency over the life of the motor. The poles on the stator ofa two-phase BLDC motor used to power a computer cooling fan.

VIII. PROPELLERS

Here in this project quad copter there arises the need of two types of propellers to need the purpose of flight. A pair of clockwise (CW) and anticlockwise (ACW) propellers is needed. The care should be taken in finalizing the dimensions of the propellers. A propeller is a type of fan that transmits power by converting rotational motion into thrust. A pressure difference is produced between the forward and rear surfaces of the air foil-shaped blade, and a fluid (such as air or water) is accelerated behind the blade. Propeller dynamics can be modelled by both Bernoulli's principle and Newton's third law. A marine propeller is sometimes colloquially known as pitch of the screw. Generally, increased propeller pitch and length will draw more current. Also the pitch can be defined as the travel distance of one single prop rotation. In a nutshell, higher pitch means slower rotation, but will increase your vehicle speed which also uses more power.

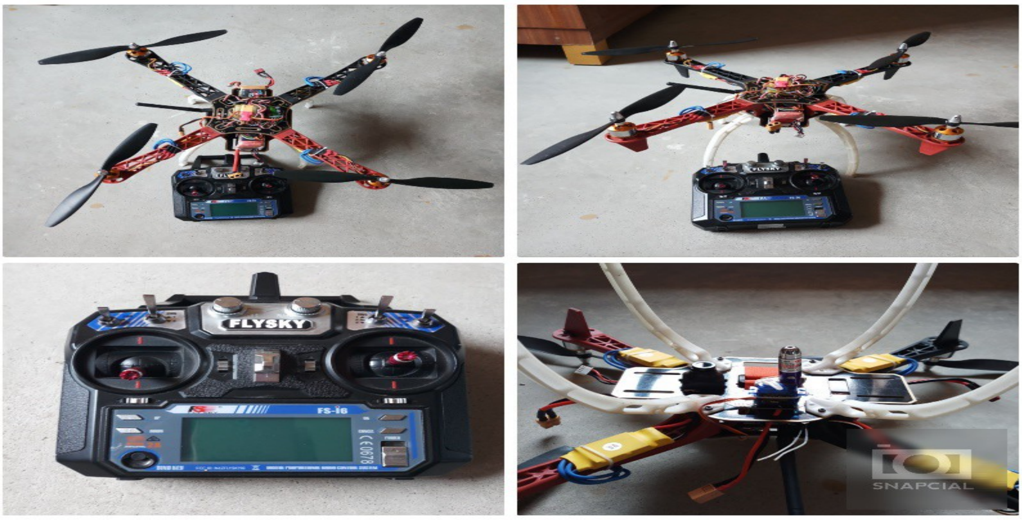
IX. FPV CAMERA

Most FPV cameras available today are primarily from the video surveillance & security industry and work very as well for FPV due to the small size and good low light capabilities. Electrical hook-up is exceedingly simple. They have 3 wire outputs (ground, power, and video signal out). Ground is usually black, power red, and video yellow. Some will also have an additional 4th wire for analog audio output if the camera also has a built in microphone (this wire is generally white). Most cameras (like the majority of the FPV video equipment on the market) are designed to operate within specific voltage ranges. The really great thing is that this range is usually in the 6 to 15VDC range making all FPV electrical components (there are some exceptions of course) operate with 2S and 3SLiPo packs without the need of special voltage regulation. It’s the 5.8 GHZ FPV camera so that it able to transmits up to 2km distances

X. XM556 MINI GUN

Xm556 is the recently launched mini gun which is operated 12v dc and it consists of 6 barrel rotary so it fire rate is aboubt (2000-6000) bullets rpm and this mini gun interfaced with quadcopter and triggered through servo respectively

XI. OUTPUT



XII. CONCLUSION

In this project we have designed the a model of intelligent drone with laser gun can be utilized by our indian army to monitor target and attack the enemies from the remote locations .

XIII. FUTURE WORK

We can provide congition capabilities to the drone so it can work completely its own intelligence without human support.

XIV. REFERENCES

1**.**S.M.Adams,C.J.Frieedland,”A survey of unmanned aerial vehicle (UAV) usage for imagery collection in

disaster research and management ,”proc.of 9th int. workshop on remote sensing for disaster response,2011

2.F.nex,F.remondino,”UAVfor3Dmappingapplication:areview”,AppliedGeomatics,vol.6,no.1 ,pp.1-15,2014

3.Department of Mechanical Engineering,University of Michigan,Ann Arbor,MI,United States.

``

Robust and Secure Video Stegnography Using Matlab

[1].J.Muthukumarasamy, [2]P.Praveenraj, [3]A.Vinayagam,
[1,2,3] UG Scholar
Department Of Electronics and Communication Engineering,
St.Anne's College of Engineering and Technology, Anguchettypalayam, Panruti

Sr.Anita.HOD/ECE
Department Of Electronics and Communication Engineering,
St.Anne's College of Engineering and Technology, Anguchettypalayam, Panruti

C.Suganya.
Assistant Professor
Department Of Electronics and Communication Engineering,
St.Anne's College of Engineering and Technology, Anguchettypalayam, Panruti

ABSTRACT: **Steganography deals with hiding text, images or video within another text, image or video file. This project focuses on secure video steganography which eliminates any suspicion to the transmission of hidden messages. This is done based on multiple objects tracking (MOT) algorithm. The hiding process is performed by concealing the secret message of all motion regions in the video depending on foreground masks. Therefore, security and robustness are provided by encoding the secret message and withstanding against various attacks.**

KEY WORDS: Video steganography, MOT, GMM, DWT, DCT

I.INTRODUCTION:

Steganography literally means covered writing. Information hiding: Utmost importance in today's world. Embedding efficiency, hiding capacity, and robustness are the three major requirements incorporated in any successful steganographic method. Data security basically aims at preserving the confidentiality and integrity of protecting data from unauthorized user or hackers. Steganography is the art of invisible communication.

The purpose is to hide very presence of communication embedding messages in third person cannot sense the presence of hidden messages. While cryptography method to conceal information by encrypting it to cipher text using unknown key and transmitting to intended receiver, the steganography provides further security in hiding cipher text into other cover medium. To hide secret information in some other source of information without leaving is to hide information in a way that prevents the detection of hidden messages.

The word steganography comes from the Greek steganos, meaning covered and any apparent evidence of data alteration steganography technology can be used.so more amount of information hides in a single video. Data containing both the cover signal and the embedded information is known as stego data.

II.BLOCK DIAGRAM:

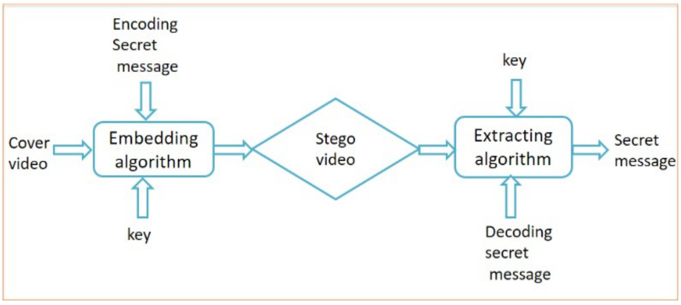


Fig. 1 General block diagram of stego method.

Cover video is a video used for hiding secret video. Secret message can be transmitted. Embedding video is a cover video + secret video + key. Stego video is nothing but a video with combine's secret messages. Then decrypt a stego video with a key Secret message can be received.

III.DWT:

DWT method is most popular method which convert digital data in the form of spatial domain into transform domain. The two- dimensional DWT is the multi resolution process. It decomposes video frame into horizontal, vertical, and diagonal sub bands using the low and high pass decomposition.

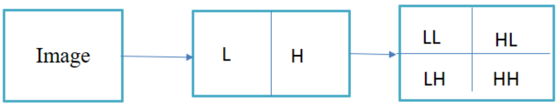


Fig 2: Process of DWT

Lo_D (z) Hi_D (z) +Lo_R (z) Hi_D (z) = 2

Lo_R (z) =zk Hi_D. (-z)

Hi_R (z) =zk Lo_D (-z)

Where Lo_D (z) and Hi_D (z) indicate the decomposition Wavelet Filters, and Lo_R (z) and Hi_R (z) represent the reconstruction wavelet filters.

DWT ALGORITHM:

Step 1: Read video.
Step 2: Convert into frames.
Step 3: Detect the motion region.
Step 4: Convert to any single plane process.
Step 5: For that plane convert to a DWT process.
Step 6: Embed that secret message with key.

Step 7: Reconstruct the video

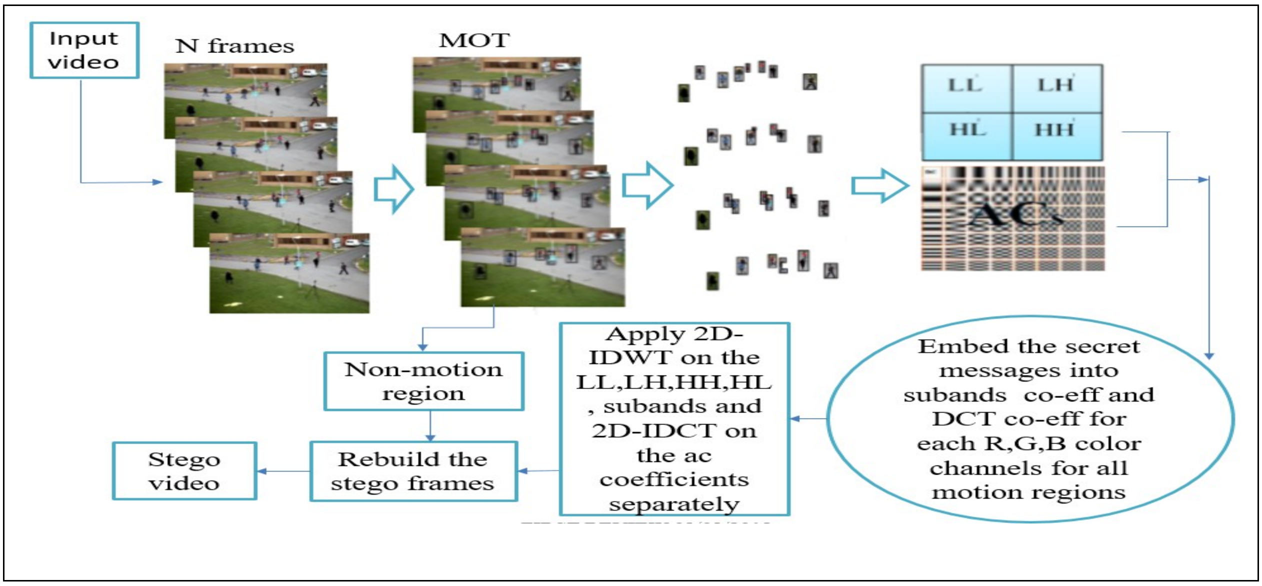

Input video
N frames
MOT
LL
LH
HL
HH
ACs
Embed the secret messages into subands co-eff and DCT co-eff for each R,G,B color channels for all motion regions
Apply 2D-IDWT on the LL,LH,HH,HL , subands and 2D-IDCT on the ac coefficients separately
Non-motion region
Rebuild the stego frames
Stego video

Fig 5: Video Steganography Framework.

IV .DCT:

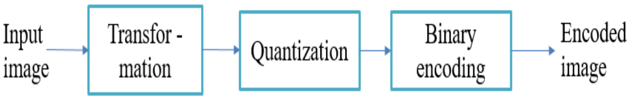


Fig 3: Process of DCT

It transforms an image from the spatial domain to the temporal domain. Image into 8 by 8 blocks and apply a 2D DCT on each block to get DC and AC coefficients. It also compress an image in a video frame.

V. MOT STAGE:

To detect and track objects moving independently to the background. and sensing of physical movement in a given area. Motion can be detected by measuring change in Speed or vector of an object.

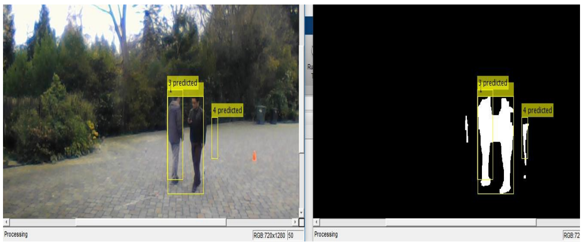


Fig 4: Motion Object Tracking

In this stage, the background subtraction technique is utilized to detect the regions of interest such as moving objects .This technique is based on the Gaussian mixture model (GMM). A Kalman filter is used to speculate the of each Trajectory.tn each video Frame, the location can each tracking is predicted by the Kalman filter more over the Kalman filter is utilized to determine the probability of a specific detection that belongs to each trajectory.

VI. DATA EMBEDDING STAGE:

Motion objects is the area of interest in each frame created. By using the motion-based MOT algorithm, the process of detecting and tracking the motion regions over all video frames are achieved. The regions of interest altered in each video frame is dependent on the number and the size of the moving objects. In every frame, 2D-DWT is implemented on RGB channels of each motion region resulting LL, LH, HL, and HH sub bands. In addition, 2D-DCT is also applied on the same motion regions generating DC and AC coefficients. Thereafter, the secret messages are concealed into LL, LH, HL, and HH of DWT coefficients, and into DC and AC of DCT coefficients of each motion object separately based on its foreground mask. Furthermore, both secret keys are transmitted to the receiver side by embedding them into the non-motion area of the first frame. Upon accomplishment, the stego video frames are rebuilt in order to construct the stego video that can be transmitted through the unsecure medium to the receiver. Algorithm clarifies the major steps of our embedding algorithm.

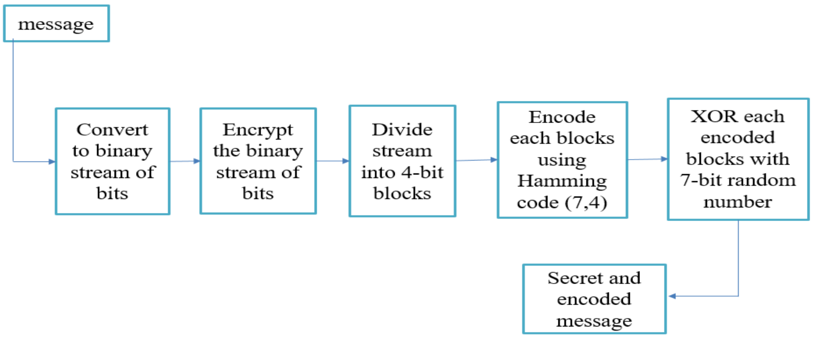

message
Convert to binary stream of bits
Encrypt the binary stream of bits
Divide stream into 4-bit blocks
Encode each blocks using Hamming code (7,4)
XOR each encoded blocks with 7-bit random number
Secret and encoded message

Fig 6: Process of input image

DATA EMBEDDING ALGORITHM:

```
Data Embedding Stage Input: V //Video, M //Secret message in characters, Key1, Key2; //Secret keys
Output: SV; //Output of Stego videos
Initialize km1, pm1, p1;
Bin ← Msm; //Change the text message to binary vector
// Stego keys
Key1 ← Len (Bin)/4; //Size of the hidden messages
Key2 ← rand (2^7, Key1, 1)'; //Randomizing the secret Key1
EnB ← En (Bin, [Key1]); //Ciphering the binary vector by Key1
For1 i = 1: (Key1*7) do //Encode each 4 bits of hidden messages by Hamming code (7, 4)
g (1:4) ← get(EnB(km1:km1+4));
En_EnB ← encode (g, 7, 4);
Item (1:7) ← get (Key2 (i));
Encdmsg (pm1:pm1+7) ← xor (En_EnB, tem);
pm1+7; km1+4;
end1
{Vf1, Vf2… Vfn} x ← V; //Video V is divided into n frames.
MODTBox ← MODT (VF); //Calling the Motion Object Detection and Tracking for each video frame VF.
Non_Motion (Vf1) ← Key1, Key2; //Embed keys (Key1 and Key2) into the non-motion areas of the first frame Vf1.
FMask = mask (VF); //Identify the foreground mask of each motion region in VF frame of size (Vfx, Vfy).
[CoeffR, CoeffG, CoeffB] ← DWT/DCT (MODTBox); //Applying 2D-DWT and 2D-DCT separately on each motion object for RGB frame components
//Conceal the secret messages into the coefficients of R, G, and B for each motion object.
```

```
For2 i = 1: Vfx do
For3 j= 1: Vfy do
If4 FMask (i, j) == 1
CoeffR1, 2, or 3 ← Encdmsg (p1+1, 4, or7);
CoeffG1, 2, or 3 ← Encdmsg (p1+2, 5, or 8);
CoeffB1, 2, or 3 ← Encdmsg (p1+3, 6, or 9);
p1+3, 6, or 9;
end4 end3 end2
SV ← {SVf1, SVf2… SVfn} x; //Obtain the stego video
```

VII.**DATA EXTRACTING STAGE:**

To recuperate the hidden images exactly the embedded video is divided into no. of frames. MOT algorithm is used to predict the route of the moving objects. After predicting the path 2D-DWT and 2D-DCT are applied to each of the moving objects and different sub bands namely LL, HH, HL and HH are created. At the extracting stage the secret messages from the LL, HH, HL and HH coefficients are retrieved and decoded by means of hamming codes.

VIII.CONCLUSION:

A robust and secure video steganography method in DWT-DCT domains based on MOT and ECC is proposed in this paper. The proposed algorithm is three-fold: 1) the motion based MOT Algorithm, 2) data embedding, and 3) data extraction. The performance of our suggested method is verified via extensive experiments, demonstrating the high embedding capacity with an average HR of 3.40% and 3.46% for DWT and DCT domains, respectively. An average PSNR of 49.01 and 48.67 dBs for DWT and DCT domains are achieved leading to a better visual quality for the proposed algorithm when compared to existing methods of the literature. The proposed algorithm has utilized MOT and ECC as the pre-processing stages which in turn provides a better confidentiality to the secret message prior to embedding phase. Moreover, through experiments from different perspectives, the security and robustness of the method against various attacks have been confirmed.

IX.FUTURE WORK:

The future scope deals with applying frequency domain techniques such as curve let transform for better security. Further this work can be extended in medical fields for secure maintenance of patient's database.

X.REFERENCES:

[1] V.swetha, V.prajith, V.kshema "Data Hiding Using Video Steganography a Survey"vol.5, Issue6, 206-213, Jun 2015.

[2] R.J.mstafa and K. M.Elleithy "A High Payload Video Steganography Algorithm in Dwt Domain Based on Bch Coded (15, 11),''in proc.wireless telecommun.symp. (WTS), Apr.2015, pp., 1-8,

[3] A. Khan, A. Siddiqi, S. Munib, and S. A. Malik, "A recent survey of reversible watermarking techniques" Information Sciences, vol. 279, pp. 251-272, 2014.

[4] A. K. Singh, B. Kumar, M. Dave, and A. Mohan, "Robust and imperceptible dual watermarking for telemedicine applications" Wireless Pers.Commun. vol. 80, no. 4, pp. 1415-1433, Feb. 2015.

[5] K. Muhammad *et al.*, A secure method for color image steganography using gray-level modi_cation and multi-level encryption," *K*SII Trans.Internet Inf. Syst., vol. 9, no. 5, pp. 1938_1962, 2015.

FORMULATION OF MATHEMATICAL MODEL FOR GABA IN DIAGNOSING EARLY PARKINSON'S DISEASE USING REGRESSION AND ARTIFICIAL NEURAL NETWORK

Sr. S. Anita,
Research Scholar,
Department Of Electronics and Communication Engineering,
SRM University.
sranitaa@gmail.com

Dr. P. Aruna Priya
Professor
Department of Electronics and Communication Engineering, SRM University,
Tamilnadu, India

ABSTRACT

Parkinson's disease (PD) is the second progressive movement disorder next to Alzheimer. The insufficiency of neurotransmitters called dopamine and Gamma-Amino Butyric Acid (GABA) in the area of human midbrain is taken as an accurate and reliable diagnostic tool to detect the disease at an early stage. The new machine learning techniques are coming out for improving the accuracy of diagnosis process. The proposed work focuses on formulating the mathematical model for predicting Parkinson's disease at an early stage based on two different machine learning strategies namely regression and Artificial Neural Network (ANN). Formulation of mathematical model uses the measured GABA concentration level as an output parameter and striatal binding ratio (SBR) values of caudate and putamen (left & right) as an input parameters. The Measured values of GABA concentration are used for finding the coefficients of the regression model and for training the feed forward back propagation neural network to calculate the predicted GABA. The variance between the measured and predicted values for regression and ANN are computed as an error rate. The neural network model was found to be capable of better predictions of PD in terms of GABA with minimum error rate.

Keywords: **Parkinson's disease, SBR, GABA concentration level, Artificial Neural Network, Prediction model**

1. Introduction

PD is a common movement disorder which disturbs human mid brain called substantia nigra. It is categorized clinically by the symptoms of resting tremor, rigidity, postural instability, bradykinesia, psychological and mental disturbances. The diagnosis of PD is easy when symptoms are full blown. However, when the disorder is mild, an accurate diagnosis is quite tough, which demands the formulation of an early detection technique for PD [1-3]. The inhibitory neurotransmitter called dopamine regulates and controls movements, motivation and cognition. Degeneration of dopamergic nerve cells along the nigrostraital pathway affects the gait system of human [4]. Thus, calculating dopamine insufficiency in caudate and putamen of the human midbrain improves the performance of diagnostic process [5, 6].

Gamma-amino butyric acid (GABA) is also a most fundamental inhibitory transmitter in the central nervous system (CNS) and spinal card. GABA mediates pre-synaptic inhibition of primary blood vessels in the motor neuron system. The disturbances of GABA concentration level of CNS influences the motor system [7]. A few neurological issues namely Parkinson's disease, anxiety, depression, insomnia, and epilepsy are connected with either low or decreased GABA concentration levels in the brain [8]. Hence, the neurotransmitters dopamine and GABA is found to be a novel diagnostic tool for detecting PD at an early stage.

In statistics, regression analysis focuses on the relationship between a dependent variable and one or more independent variables. Primarily, it supports to understand how the dependent variable changes when any one the independent variable is changed, while the other independent variables are held fixed. When regression analysis has substantial overlap with the field of machine learning, it is used to predict the various disorders. It is also used to realize how the independent variables are related to the dependent variable and to investigate the forms of these relationships [9]. The machine learning techniques such as Multivariate Logistic Regression (MLR), Support Vector Machine (SVM), and Artificial Neural Network (ANN) are used effectively to formulate a prediction model for diagnosing neural disorders. Machine learning techniques consent with individual level characterization rather than at group level. Hence, high level of clinical translation is obtained. SVM finds hyper plane to classify the subjects. MLR aims to determine the probability based on SBR values, which classify the subjects into different risk categories [10-12].

Recently the Artificial Neural Network is used as a prediction model for diagnosing various diseases in different medical areas [13]. It has weighted-interconnected nodes called stimulated neurons and has the ability of human brain to control overall activities of the network. It experiences from the past experiences and find solutions for complex nonlinear multidimensional functional relationships. The unique characteristic of ANN is to train the network from a large number of inputs without prior knowledge about the problem. The trained network classifies and tests the dataset based on training strategy. The three layered back propagation with levenberg-marquardt (LM) training algorithm in ANN serves as an effective, simple, fast and efficient tool for predicting various properties of the materials [14-16]. In the related work [17], huge number of features are used, which requires an effective feature reduction techniques like principal component analysis (PCA), independent component analysis (ICA) to pick up the required features. This technique complicates the system design.

The present work organizes as follows. Section 2 contributes about materials and the theory behind the proposed system. Section 3 gives the mathematical model for PD and healthy control (HC) using regression and ANN, estimation of error rate and their description. Finally conclusion has drawn in section 4.

2. Computational Methodology

2.1 PPMI Database

The SBR values of PD and HC are taken as input parameters and are obtained from Single-photon emission computed tomography (SPECT) image of the international Parkinson Progression Marker Initiative (PPMI) database. All PD subjects included in the database are in an early stage of the disease based on Hohen and Yahr stage 1 and 2 or two years or less [18].

2.2 *Calculation of SBR values*

SPECT raw projection data was reconstructed using hybrid ordered subset expectation maximization (HOSEM) algorithm. Iterative reconstruction was done without any filtering to ensure consistency of the reconstructions. The same anatomical alignment was obtained by Attenuation correction, filtering and normalization. Striatal uptake count densities of the region of interest (ROI) were extracted and used to calculate striatal binding ratios (SBRs) for each region of the four striatal regions.SBR is calculated by PPMI as follows, and considered an occipital cortex region as reference region, which is located below Putamen [19].

$$\text{SBR}= (\text{target region}/\text{reference region}) - 1 \qquad (1)$$

Where,
Target region: left caudate, right caudate, left putamen,right putamen.
Reference region: occipital cortex.
Table 1 shows the number of observations and averaged SBR values.

Table 1: Averaged SBR value for caudate right & left, putamen right & left for Early PD and HC

Cases	No. of observations	Caudate(R)	Caudate(L)	Putamen(R)	Putamen(L)
Early PD	360	1.91	1.87	0.810	0.729
Healthy control	163	2.96	3.07	2.16	2.23

2.3 Regression Analysis

Regression analysis is a statistical tool for the exploration of the relationship between variables that is used for interpreting or modeling the relationship between a single variable Y, called the response, output or dependent variable and one or more predictor, input, independent or explanatory variables, X_1 . . . . . . Xp.
The general form of the linear regression equation is:

$$Y = a + bX \qquad (2)$$

Where, Y= Variable to be predicted; X= Variable used to predict Y; a = the intercept; b = the slope.
Regression analysis for developing the mathematical models of PD and HC was carried out using the statistical package Minitab ver15. Here, regression is used to estimate the qualitative effect of the input variables namely caudate left & right and putamen left & right upon the output variable GABA [20]. The standard error (SE) of regression indicates that the observations are closer to the fitted line, and the following equation calculates it.

$$\text{SE of regression} = \frac{\sqrt{\Sigma(yi - \hat{y}i)2}}{\Sigma(xi - x)2} \qquad (3)$$

Where,
yi is the value of the output for observation i, ŷi is estimated value of the output for observation i, xi is the observed value of the input for observation i, x is the mean of the independent variable, and n is the number of observations. The p-value for each term checks the null hypothesis that the coefficient is equal to zero (no effect). A low p-value (< 0.05) demonstrates that the model is significant. And a high P-value (>0.05) shows that the model is insignificant. The coefficient of determination (R-squared) is a statistical measure of how close the data are in the fitted regression line. R-squared is always between 0 and 100%. 0%

indicates that the model defines none of the variability of the output data around its mean. 100% point out that the model defines all the variability of the output data around its mean. In general, higher the R-squared, the model fits with the data efficiently [21].

2.4 ANN architecture

Artificial neural network architecture is a supervised learning architecture, which consists of a various number of layers as shown in fig. 2. (1) Input layer where the input patterns are applied, (2) output layer where the output is obtained, and the (3) hidden layers (i.e., layers between the input and output layers) as in fig.2. Hidden layers are so named because their outputs are not directly visible. In addition, the hidden layers allow the network to extract higher-order statistics, which are particularly valuable when the size of the input layer is large [22, 23]. Neurons of each layer are interconnected to the neurons of preceding and subsequent layer with associated weighted connection.

The input signal communicates the signal throughout the network in a forward direction, on a layer-by-layer basis. These networks are commonly referred as multilayer perceptron (MLP) [24]. The hidden layers serve: (i) add non-linearity to the system and (ii) address interactions between input variables. There are many hidden layers, i.e. many levels of nonlinearity and interactions. The selection of the number of hidden layers is the most important factor to be considered while solving a problem.

2.5 Implementation

In the present investigation, an ANN was modeled using a NF tool box of MATLab®. NF tool is a network fitting tool with graphic user interface (GUI) unit. The data were divided into training sets, validation set and testing set in the proportions of 70:15:15 respectively. The network was trained by using Levenberg-Marquardt back propagation (LMBP) algorithm, with Mean Square Error (MSE) as the performance measuring the parameter.

The back propagation neural network was modeled based on delta rule, called steepest descent algorithm. It consists of a forward pass of input, hidden and output training samples. A backward pass of the sample is made to update the weight ω_{ij} of all neurons *i* in layer *k*. One epoch is presented to the network when a forward pass and backward pass have made. The forward pass output will be

$$\zeta_k(n) = \sum_{j=0}^{m} \omega_{kj}(n)\gamma_j(n) \tag{4}$$

Where *n* – No of conducted epochs
k- No of layers
ω- Current weight vector
m- No of neurons in layer k
$\gamma$is the output vector from the previous defined as

$$\gamma_j(n) = \alpha_j(\zeta_j(n) \tag{5}$$

The error in the forward pass output layer is represented as the difference between the predicted value and the desired value d as the overall squared error.

$$\epsilon_k(n) = \frac{1}{2}\sum_{j=0}^{m}[d_j(n) - \gamma_j(n)]^2 \tag{6}$$

Differentiating ε with respect to ε_j , the delta rule is obtained as

$$\Delta\omega_{kj}(n) = -\eta\frac{\partial\epsilon(n)}{\partial\omega_{kj}(n)} \tag{7}$$

Where η is defined as learning rate

The modified steepest descendent rule is used as LM training algorithm. The LM is the faster and more accurate algorithm with minimum error, when compared to the steepest descendant rule. The error function is given with a Taylor expansion

$$\in (n+\delta) = \varepsilon(n) + J(n).\delta \tag{8}$$

Where J(n) is the Jacobian matrix [21, 25].

In this study, the four neurons input layer represents four variables like caudate left & right and putamen left & right, 30 neurons with log-sig activation function hidden layer and one neuron output layer is used to design the network to predict GABA concentration level for PD and HC.

3 Result and discussion

3.1 Statistical modeling

The coefficients of regression analysis of GABA concentration level for PD and HC is shown in table 2 along with their significant (P) value of the parameters. From the table, the P value of regression analysis of GABA for caudate left and putamen left are most significant, whereas caudate right and putamen right are not so significant for PD, which indicates less discriminating power than other parameters.

Table 2 Regression Table of GABA for PD and HG

Predictor	B		SE		T		P value	
	PD	HC	PD	HC	PD	HC	PD	HC
Constant	0.114468	-1.55259	0.005631	0.05426	20.33	-28.61	0.00	0.000
Caudate(R)	0.008960	0.04483	0.004785	0.02168	1.87	2.07	0.062	0.040
Caudate(L)	0.025654	0.17483	0.004956	0.02208	5.18	7.92	0.000	0.000
Putamen(R)	-0.005756	-0.01417	0.006367	0.02330	-0.90	-0.61	0.367	0.544
Putamen(L)	-0.028090	0.75694	0.007518	0.02579	-3.74	29.35	0.000	0.000

B is a regression coefficient for the predictors; SE is its standard error; T is test statistics; P value is the significance of the regression coefficient;

Similarly, for HC caudate right, caudate left and putamen left are the most significant, whereas putamen right is not most significant. The regression model equation of GABA concentration level for PD and HC is given in equation 9 & 10.

GABA (PD) = 0.114 + 0.00896 × Caudate(R) + 0.0257 × Caudate (L) - 0.00576 × Putamen (R)- 0.0281 × Putamen (L) (9)

GABA (HC) = - 1.55 + 0.0448 × Caudate(R) + 0.175 × Caudate (L) - 0.0142 × Putamen (R) + 0.757 × Putamen (L) (10)

Where S is the estimated standard deviation about the regression line, R-squared also called the coefficient of determination. Adjusted R-squared is an approximately unbiased estimate of the population R-squared. The S value is the measurement of error it is smaller the better. The higher value of R-squared is smarter to define the coefficients of a regression equation. The nearness of the adjusted R-squared with R-squared decides the fitness of model [16]. In both cases, the adjusted R-squared value is very nearer to the R-squared value is shown in table 3.

Table 3 Summary of regression analysis

Responses	S value	R^2 (%)	Adjusted R^2 (%)
GABA for PD	0.0248413	99.3	98.7
GABA for HC	0.108489	95.3	94.2

S is the standard deviation; R^2 is the coefficient of determination; Adjusted R^2modified version of R^2

A high value of the determination coefficient confirms model adequacy, the goodness of fit and high significance of the model. This shows that the regression models for the output can be used for determining and valuing GABA for PD and HC.

An analysis of variance (ANOVA) was performed for GABA for PD and healthy group are presented in table 4. The associated p-value for both the models is lower than 0.05 (i.e. level of significance α=0.05, or 95% confidence), which indicates that both (PD and HC) the models can be considered statistically significant [21].

Table 4 Analysis of Variance for PD and HC

Source	DF		SS		MS		F		P value	
	PD	HC	PD	HC	PD	HC	PD	HC	PD	HC
Regression	4	4	0.059270	37.8153	0.014818	9.4538	24.01	803.22	0.000	0.00
Residual Error	355	158	0.219067	1.8596	0.000617	0.0118				
Total	359	162	0.278338	39.6750						

DF is the degrees of freedom; SS is Sum of Squares; MS is Mean Squares; F calculated F value; P is a significance of regression coefficient.

Figure 2 and 3 shows the residual values with the fitted values for GABA for PD and HG. Figure 2 indicates that the maximum variation of -0.075 to 0.050, which shows the high correlation that exists between fitted values and observed values.

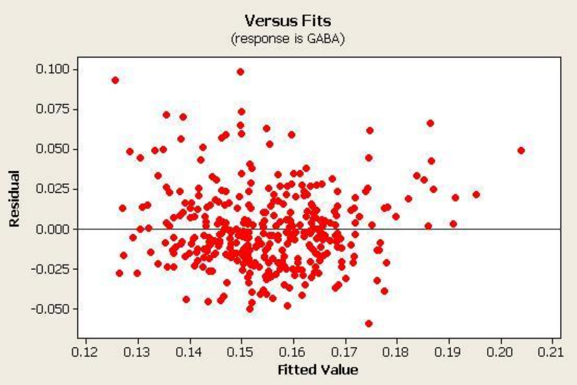


Fig. 2 Residual Vs fitted values for GABA for PD

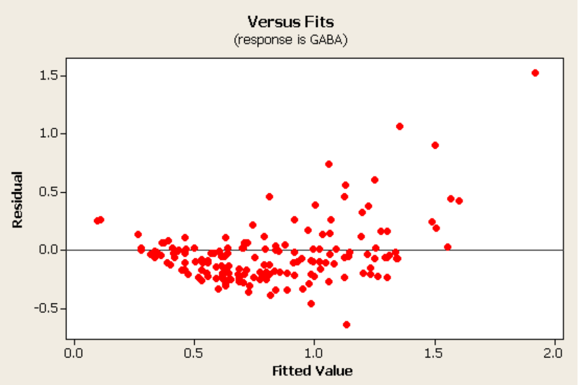


Fig. 3 Residual Vs fitted values for GABA for HG

3.2 Artificial Neural Network

3.2.1 Effect of SBR values on GABA concentration level for PD

Based on the SBR values of Caudate (L), Caudate (R), Putamen (L) and Putamen (R) the predictive model of GABA concentration level for PD is developed by ANN. Regression plot is drawn to learn the error and accuracy. Fig.4 shows the regression plot for PD. The plot shows the average regression value (R= 0.99954) is very near to 1, which means that the predicted values are very close relationship with the output as the data in the graphs lie on the fit. The same can be appreciated for training, testing and validation individually.

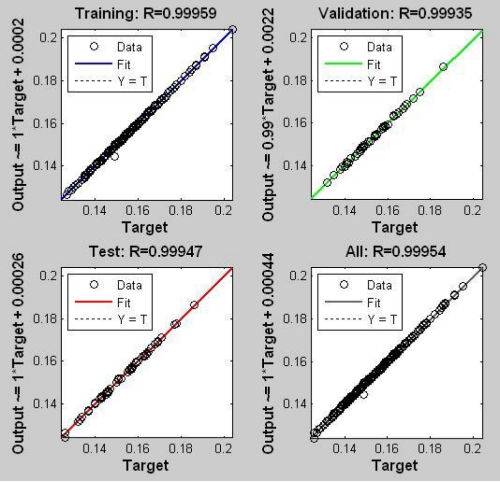


Fig. 4 The regression plots of training, testing, validation and average of all sets for PD

3.2.2 Effect of SBR values on GABA concentration level for HG

Similarly, based on the SBR values of Caudate (L), Caudate (R), Putamen (L) and Putamen (R) the predictive model of GABA concentration level for HG is developed by ANN. Regression plot is drawn to study the error and accuracy. Fig.5 shows the regression plot for HG. The plot shows the average regression value (R= 0.9981) is very close to 1, which means that the predicted values are very near relationship with the output as the data in the graphs lie on the fit. The same can be appreciated for training, testing and validation individually [21].

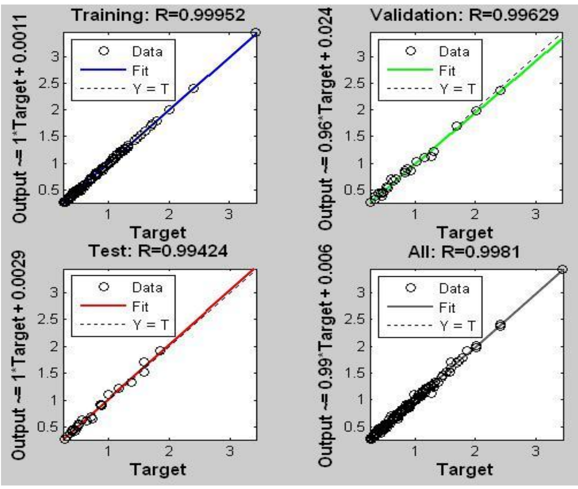


Fig. 5 The regression plots of training, testing, validation and average of all sets for HG

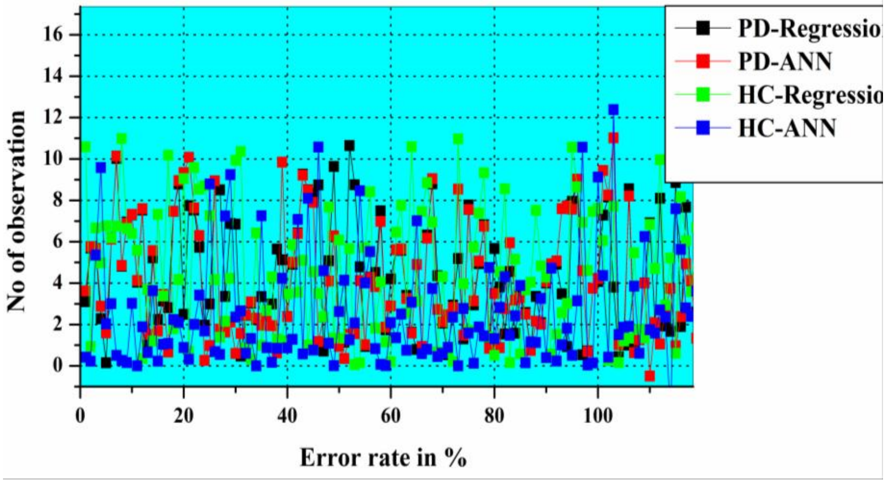
3.3 Calculation of error rate

The difference between measured and predicted value of GABA concentration is estimated for regression and ANN. Table 5 displays the validated results of the proposed method in terms of Mean, SD, Min and Max. values. It is observed from the table that ANN has the error rate of 4.0021 for PD and 2.743237 for HC, which ensures that the ANN model produce minimum error rate and SD compared to other models. The above results are ensured by the comparative error rate for ANN and regression analysis shows in Fig. 6.

Table 5 Descriptive Statistics values of error in percentage

	N	Min. (%)	Max. (%)	Mean (%)	SD (%)
PD Regression	360	.04281676928942	19.9681495152803	4.550959427393	3.301557782589
PD ANN	360	.01070801358824	12.8841509870642	4.002100322772	2.8242759615544
HC Regression	163	.05868612176485	18.276064058796	4.831238659379	3.3135857354786
HC ANN	163	.00041715485883	12.3859573710988	2.743237373447	2.696838671208

N- no. of observation, Min- Minimum, Max- Maximum, SD- Standard deviation



4 CONCLUSIONS

In this study, the application of regression analysis and neural network analysis on the experimental surface roughness values are compared and discussed. In this study, the application of regression analysis and neural network analysis on the experimental surface roughness values are compared and discussed. The formulation of mathematical model for PD and HC using regression analysis and artificial neural network analysis of GABA concentration level are compared and discussed. It is found to be a close correlation with the results of regression and ANN. The coefficient of determination (R^2) of PD and HC was 0.993 and 0.953 in the regression model. The ANN model with 20 hidden layer neurons has created R^2 values of 0.99959 for the training data, and 0.99947 for the test data of PD and 0.9995 for the training data, and 0.99424 for the test data of HC. The neural network model indicates better predictions than various regression models for GABA concentration level. However, both methods can be used for the prediction of GABA concentration level with minimum error.

References

[1] De Lau, L. M and Breteler, M. (2006) 'Epidemiology of Parkinson's disease', The Lancet Neurology, vol. 5, pp.525-535.

[2] Moore DJ, West AB, Dawson VL, Dawson TM. “Molecular pathophysiology of Parkinson's disease.” Annual Review Neuroscience 28 (2005): 57-87.

[3] Prashanth , R., SumantraDutta Roy Pravat and. MandalShantanuGhosh, K. (2014)'Automatic classification and prediction models for early Parkinson’s disease diagnosis from SPECT imaging',Exepert system with Applications vol. 41, pp.3333-3342

[4] T .C. Booth.M, Nathan.A.D.waldman.A.Mquigley, A.H.Schapuria and J. Buscombe “The role of functional dopamine transporter AJNR AMJ neuroradial 36:229-35, Feb 2015

[5] Bairactaris, C., Demakopoulos, N., Tripsianis, G., Sioka, C., Farmakiotis, D., Vadikolias, K., Heliopoulos, I., Georgoulias, P., Tsougos, I., Papanastasiou, I., & Piperidou, C. (2009). ‘Impact of dopamine transporter single photon emission computed tomography imaging using I-123 ioflupane on diagnoses of patients with parkinsonian syndromes’, Journal of Clinical Neuroscience, vol.16,pp. 246-252.

[6] Booij, J., Tissingh, G., Boer, G. J., Speelman, J. D., Stoof, J. C., Janssen, A. G., Wolters, E. C., & van Royen, E. A. (1997) ' [123I]FP-CIT SPECT shows a pronounced decline of striatal dopamine transporter labeling in early and advanced Parkinson's disease', Journal of Neurology, Neurosurgery & Psychiatry, vol. 62, pp.133-140.

[7]Pellicano,C.,Benincasa,D.,Pisani,V.,Buttarelli,F.R.,Giovannelli,M.,andPontieri,F.E.(2007). Prodromalnon-motor symptoms of Parkinson's disease.Neuropsychiat.Dis.Treat.3,145–152.doi:10.2147/nedt.2007.3.1.145

[8] (2007)'American college for advancement in medicine', Monograph, Alternative Medicine Review, Vol 12, pp-274-279

[9] Douglas C. Montogomery, Elizabeth A. Peck and G.Geoffrey Vining (2001) 'Introduction to Linear Regression Analysis' Arizona State University, fifth edition,576 pages.

[10] Orru, G., Pettersson-Yeo, W., Marquand, A. F., Sartori, G., & Mechelli, A. (2012). Using support vector machine to identify imaging biomarkers of neurological and psychiatric disease: a critical review. Neuroscience &Biobehavioral Reviews, 36, 1140–1152.

[11] Shubhambind, Arvind Kumar Tiwari, Anil Kumar Sahani, (2015). A Survey of Machine learning Based Approaches for Parkinson Disease prediction, vol 6 (2),1648-1655

[12] Winogrodzka, A., Bergmans, P., Booij, J., van Royen, E. A., Janssen, A. G., & Wolters, E.C. (2001). [123I]FP-CIT SPECT is a useful method to monitor the rate of dopaminergic degeneration in early-stage Parkinson's disease. Journal of Neural Transmission, 108, 1011–1019.

[13] Rasit Koker, Necat Altinkok and Adem Demir, "Neural network based prediction of mechanical properties of particulate reinforced metal matrix composites using various training algorithms", Materials &amp; Design, Vol. 28, pp 616-627, 2007.

[14] Zhenyu Jiang, Zhong Zhang and Klaus Friedrich, "Prediction on wear properties of polymer composites with artificial neural networks", Composites Science and Technology, Volume 67, Issue 2, Pages 168-176, February 2007.

[15] H. S. Rao and A. Mukherjee, "Artificial neural networks for predicting the macromechanicalbehaviour of ceramic-matrix composites", Computational Materials Science, Volume 5, Issue 4, Pages 307- 322, April 1996.

[16] Mehmet Sirac Ozerdem, Sedat Kolukisa, "ANN approach to predict the mechanical properties of Cu–Sn–Pb–Zn–Ni cast alloys", Materials and Design, 30, 764–769, 2009.

[17] Rojas, A., Górriz, J. M., Ramírez, J., Illán, I. A., Martínez-Murcia, F. J., Ortiz, A., et al. (2013). Application of empirical mode decomposition (EMD) on DaTSCAN SPECT images to explore Parkinson disease. Expert Systems with Applications, 40, 2756–2766.

[18] Francisco P M Oliveira, and Miguel Castelo-Branco, (2015) 'Computer-aided diagnosis of Parkinson's disease based on [123I]FP-CIT SPECT binding potential images, using the voxels-as-features approach and support vector', J. Neural Eng. Vol. 12 (10pp) doi:10.1088/1741-2560/12/2/026008.

[19] Seibyl, J. Jennings, D.. Grachev, I. Coffey, C and.Marek, K , (2013) '123-I Ioflupane SPECT Measures of Parkinson Disease Progression in the Parkinson Progression Marker Initiative (PPMI) Trial', in Society of Nuclear Medicine Annual Meeting Abstracts, pp. 190.

[20] Julian J. Faraway, (2002) 'Practical Regression and ANOVA using R' first edition,210 pages.

[21] S. Anita and P. ArunaPriya," Early Prediction of Parkinson's Disease using Artificial Neural Network", Indian Journal of Science and Technology, Vol. 9(36), DOI: 10.17485/ijst/2016/v9i36/98401, September 2016

[22] Schalk off RJ. "Artificial neural networks", McGraw-Hill; 1997.

[23] S. Kumar Chandar, M. Sumathi, S. N. Sivanandam,"Prediction of Stock Market Price usingHybrid of Wavelet Transform and Artificial Neural Network",Indian Journal of Science andTechnology,2016 Feb, 9(8), Doi no:10.17485/ijst/2016/v9i8/87905

[24] S. Rajasekaran and G.A.VijayalakshmiPai, "Neural networks, fuzzy logic and genetic algorithms synthesis and application" Prentice-Hall of India Pvt., Ltd, New Delhi, 2004.

[25] Freddie Astroma, Rasi t Kokerb.C, A parallel neural network approach to prediction of Parkinson's disease, Expert Systems with Applications 38, 2011, 12470–12474

[26] S. Anita and P. Aruna Priya, "Estimation of Parkinson's disease risk by statistical mod" in the journal of Institute of Integrative Omics and Applied Biotechnology (IIOAB), Vol. 8(3), pp. 42-48, 2017.

Analysis and Design of Circular Microstrip Patch Antenna for ISM Band Applications

Mr. S. DURAI RAJ
Assistant Professor,
Department of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Mr. V. VENKATESAN
Assistant Professor,
Department of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Abstract*— Here we made an attempt to maximize the gain of microstrip patch antenna. To achieve this we used microstrip circular patch antenna at 5.8 GHz frequency ISM Band Application. Single FSS (frequency selective surface) substrate is used to increase efficiency. Parameters are set accordingly microstrip patch antenna with substrate layer on the basis of return loss, directivity, radiation pattern and gain. We used HFSS (high frequency structured simulator) software for simulation of antenna and to find out the results. We keep changing the design of antenna as our motive was to achieve miniature antenna with better results than conventional antenna's. Thickness of substrate has been minimized to achieve the same. Coaxial feeding technique has been used as it is easier to implement.

***Keywords*— Microstrip Antenna, Operating frequency 5.8GHz, Circular Microstrip patch antenna**

I.INTRODUCTION

Microstrip antennas are divided into 4 different categories they are:

- Microstrip Patch antenna
- Microstrip dipoles
- Printed slot antennas
- Microstrip travelling wave antenna

Within few years microstrip patch antenna has gained lot of popularity and considered as most dynamic field in communication and being used to realize millimeter wave monolithic integrated circuits for microwave, radar, GPS antennas and communication purposes. In response to their increasing demand for compact and easy fabricated antenna with efficient results for use in various wireless communication systems, several circular antennas have been developed over the past decade. The major disadvantages of these antennas are narrow bandwidth and gain. Advantages of these Antennas are its low profile, robustness, inexpensive, light and compact design. Photo etching technology is used to fabricate antenna together with microwave circuit. It supports both linear as well as circular polarization.

FSS (frequency selective surface) has a structure of periodically arranged array of special element in print on a substrate. As mentioned previously, FSS structures are periodic arrays of special elements in print on a substrate.

A feeding technique is a way to supply radio waves into the antenna structure. Number of feeding technique is in use in the technologies, it can be contacting and Non contacting. The criteria of division are direct and indirect connectivity of RF (radio Frequency) power supply with the antenna. Microstripline and coaxial are contacting feeding technique whereas aperture and proximity is non contacting feeding.

Here simulated result of circular patch antenna with single FSS layer compared with circular patch antenna without FSS layer. Details of both the antennas design and simulation result are presented and discussed.

II.RELATED WORK

Microstrip patch antennas have larger application due to its low profile, light weight, and ease to fabrication but with this there are few disadvantages as well i.e. low gain and narrow bandwidth. Many techniques have been applied to enhance the impedance bandwidth. Different feeding technique, use of FSS substrate, patch design they are the few ways that significantly reduces the losses. DNG (Double Negative Slab), dielectric Slab and FSS are being used better efficiency is achieved using dielectric [2]. With the simulation theoretical calculation is also done and being compared with simulation results. It shows nearby results as in [4] it achieved 3.3% bandwidth 4.2 dB gain.

Spacing between the substrates is filled with air and right decision of air gap has to be maintained to achieve best results. At the ISM band frequency 5.8GHz which achieved greater than 5 dB and showed conical radiation [8]. Similarly, another paper has demonstrated antenna at same frequency which achieved bandwidth 12.8% and gain of 5.7 dB [10].

Use of substrate is another way to get better results and even to reduce the size of antenna. Fractal shapes using Koch has reduced the size of antenna up to 80.3% [14].

III.ANTENNA DESIGN ANALYSIS

Microstrip patch antenna is used at 5.8GHz as resonance is achieved at this point. Coaxial feeding technique is used in the design because of its feature that it is easy to obtain input matching by adjusting feed position. Input impedance matching is critical requirement to achieve required bandwidth, if it doesn't occur than efficiency will be lower. "Line fed rectangular patches may be fed from the radiating or the non -radiating edge. To find an impedance match along the non-radiating edge we may use the Transmission Line Model.

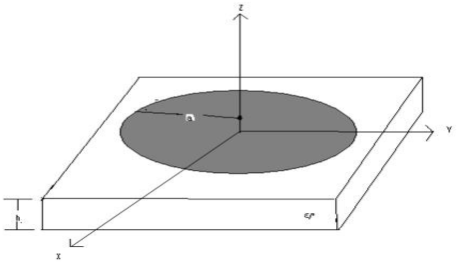


Fig.3.1.Geometry of Circular Patch Antenna

A. *Method of Analysis*

Wavelength in free space λo: c/ fo c is the velocity of light in air.

Therefore the resonant frequencies for the TMmn0 modes can be written as (Richards, 1988; Gonca, 2005)

$$(f_r)_{mn0} = \frac{1}{2\pi\sqrt{\mu\varepsilon}}\left(\frac{X'_{mn}}{a}\right)$$

Circular patch radius:

$$a = \frac{F}{\left\{1+\frac{2h}{\pi\varepsilon_r F}\left[\ln\left(\frac{\pi F}{2h}\right)+1.7726\right]\right\}^{1/2}}$$

$$(f_r)_{110} = \frac{1.8412 v_0}{2\pi a_e\sqrt{\varepsilon_r}}$$

Effective radius of circular patch:

$$a_e = a\left\{1+\frac{2h}{\pi\varepsilon_r a}\left[\ln\left(\frac{\pi a}{2h}\right)+1.7726\right]\right\}^{1/2}$$

TABLE 1

ANTENNA DESIGN SPECIFICATION

PARAMETER	VALUES
Frequency band used	ISM band
Operating frequency :	5.8GHz
Wavelength in free space/ vacuum	51.72mm
Radius of circular patch	9.88mm
Substrate dielectric material	RT-duroid 5880
Substrate dielectric constant	2.2
Substrate thickness:	0.762mm
FSS surface used in superstrate layer above direction	FR-4 epoxy (4.4)(R= 2.5mm)
FSS surface used in below direction	RT duroid 5880
Feeding technique	probe feeding
Feed point location from center	3.1mm
Air gap	28.96(0.56 * 51.72mm)
Ground plane	l=75mm, W= 75mm

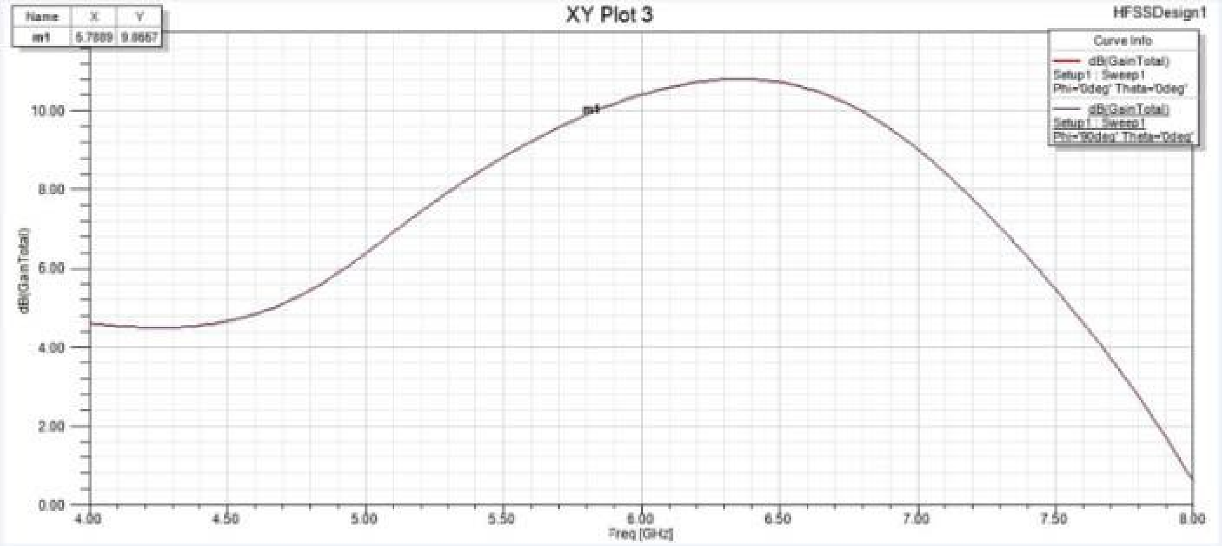
IV.SIMULATION RESULT AND DISCUSSION

Result of Microstrip Patch Antenna with Single FSS Layer:

1) Total Gain:

Operating Frequency: 5.8GHz Value of Gain Total (in db):9.8557
Peak point (m1) of operating frequency: 5.7889GHz

Figure.4.1 Total gain (db) with single FSS



2) Radiation Pattern:

Operating frequency: 5.8GHz
Setup1: sweep1
Peak point (m1) of operating frequency: 5.7889GHz Phi (in degree)-0 degree, phi (in degree) = 90 degree

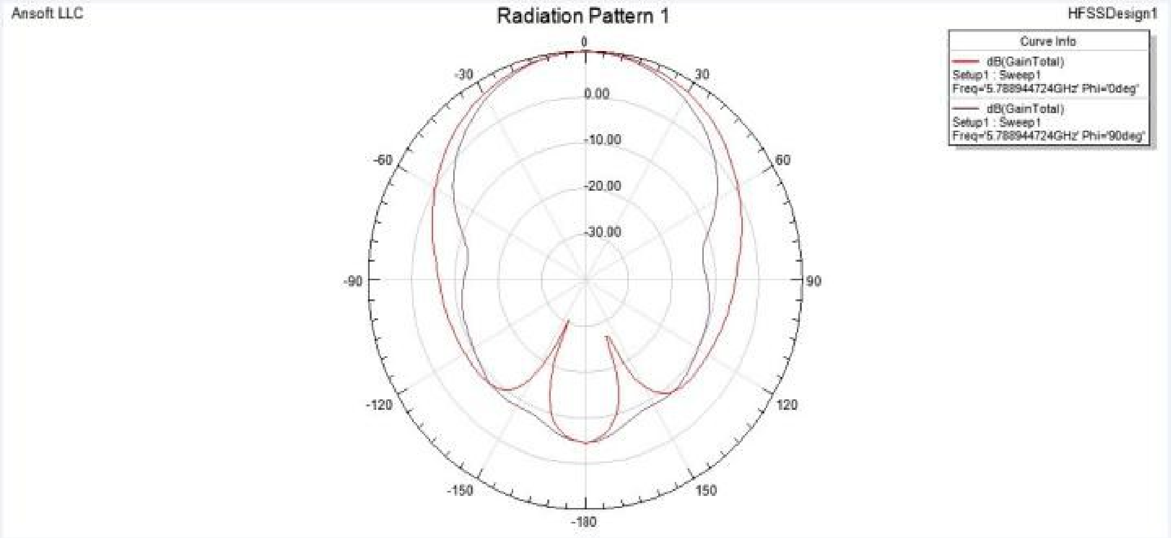


Figure.4.2 Radiation pattern with single FSS

3) Return Loss:

Operating frequency: 5.8GHz
Value on return loss: -14.7357db
Peak point of operating frequency: 5.7688GHz

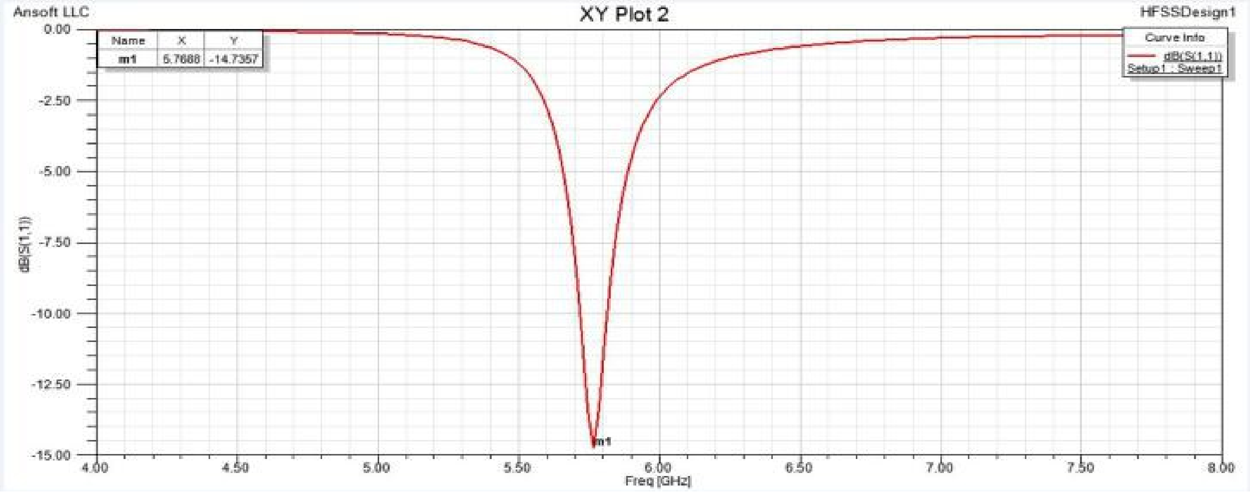


Figure.4.3 Return loss (db) with single FSS

4) Directivity:

Operating frequency: 5.8GHz
Setup1:Sweep1
Peak point (m1) of operating frequency: 5.7889GHz Phi (in degree) = 0 degree, phi (in degree) = 90 degree

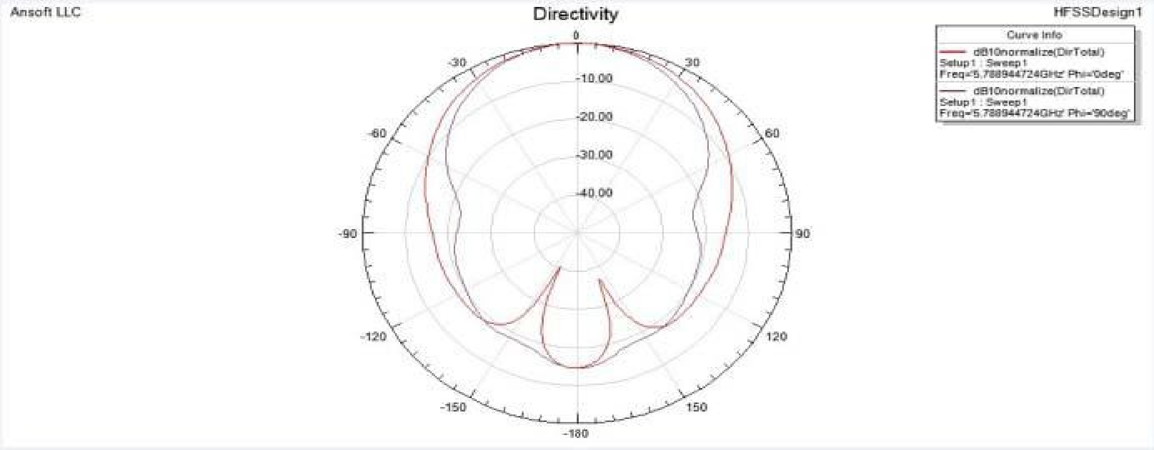


Figure.4.4 Directivity with single FSS

V.CONCLUSION:

We made analysis circular microstrip patch antenna which achieved resonance at 5.8GHz with FR-4 epoxy single layer with permittivity (r =4.4) gives 38% increase in gain. The antenna radiation reflected lesser in antenna with FSS layer by 7.17% in reduction of return losses.

REFERENCES:

1. Carver, Keith R., and James Mink. "Microstrip antenna technology." Antennas and Propagation, IEEE Transactions , pp 2-24, Feb 1981
2. Gohil, J.V.; Bhatia, D., "Design of 2×1 circularly polarized microstrip patch antenna array for 5.8 GHz ISM band applications," Engineering (NUiCONE), 2012 Nirma University International Conference in Ahmadabad, IEEE Publisher on, pp.1-4, 6-8 Dec. 2012.
3. Mittra, R., Li, Y. and Yoo, K "A comparative study of directivity enhancement of microstrip patch antennas with using three different superstrates" Microwave Optical Technology Letter, volume 52, issue 2, 327–331, Feb 2010.
4. Gupta, Samir Dev, and Amit Singh. "Design And Analysis Of Multi dielectric Layer Microstrip Antenna With Varying Superstrate Layer Characteristics." International Journal of Advances in Engineering & Technology, Vol. 3 Issue 1, p55-68. 14p, Mar 2012.
5. T. F. Lai, Wan Nor Liza Mahadi, Norhayatision, "Circular Patch Microstrip Array Antenna for KU-band", World Academy ofScience, Engineering and Technology, vol. 48, pp. 298-302, 2008.
6. A.Kotrashetti, J.Anthony, H. Crasto, N.Ram "Design and development of microstrip patch antenna for ISM band transmitte rreciever system" in proceeding of international conference and Workshop on Emerging Trend in Technology, ACM New York, Pages 458-461, Feb 2010.
7. Z.-W. Yu, G.-M. Wang, X.-J. Gao, and K. Lu, "A novel small-size single patch microstrip antenna based on koch and sierpinski fractalshapes," Progress In Electromagnetics Research Letters, Vol. 17, 95- 103, 2010.
8. Keshav Gupta et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3895-3898

Alive Human Detection Robot in Rescue Operation

Ms.S.Aayisa Banu
UG Scholar,
Department of Electronics and Communication Engineering,
V.R.S. College of Engineering and Technology,
Arasur-607017, Tamil Nadu.

Ms.D.Vishnupriya
UG Scholar,
Department of Electronics and Communication Engineering,
V.R.S. College of Engineering and Technology,
Arasur-607017, Tamil Nadu.

Ms.L.Sasina
UG Scholar,
Department of Electronics and Communication Engineering,
V.R.S. College of Engineering and Technology,
Arasur-607017, Tamil Nadu.

Mr.V.Thiyagarajan
Associate Professor,
Department of Electronics and Communication Engineering,
V.R.S. College of Engineering and Technology,
Arasur-607017, Tamil Nadu.

Abstract — Many areas of the world get affected by natural calamity. Disasters are unstoppable and leave behind a great loss of life. Disasters like earthquake, floods, etc. cause mass destruction and often lives get buried or trapped in debris. In such situations detection by rescue workers becomes time consuming and due to the vast area that gets affected it becomes more difficult. Hence, we are proposing a human detection robot which can detect alive humans in debris so that timely help can be made available to the victims. The robot is equipped with a PIR sensor to detect live human, a robotic arm to remove any obstacles in its way, a camera to send images to control unit. Microcontroller SST89E516RD is used to control the robot and is the core of robot. The robot consists of a three wheel geared drive with DC motors attached to perform forward and reverse movements.

***Index Terms*— Calamity, debris, PIR sensor, robotic arm, control unit, DC motor.**

I. INTRODUCTION

A timely rescue can only save the people who are buried and wounded due to a disaster. In such situations, rescue system must take fast decisions under pressure, and try to get victims to safe location at their own risk. The rescue system must collect the location information and status of victims as quickly as possible so that medication and fire-fighters can enter the disaster prone area and save people. All these works are performed mostly in very dangerous and risky situations by human and trained dogs. Detection by rescue workers becomes time consuming and due to the vast area that gets affected it becomes more difficult [3]. So the project proposes a mobile rescue robot that moves in a disastrous area and helps in identifying the live people and rescue operations. A robot is a reprogrammable, multifunctional manipulator designed to move materials, parts, tools or specialized devices through variable programmed motions for the performance of a variety of tasks. Basically a robot consists of a mechanical structure, such as a wheeled platform, arm, or other construction, capable of interacting with its environment. Sensors are used to sense the environment and give useful feedback to the device. Systems to process sensory input in the context of the current situation and instruct the device to perform actions in response to the situation [2]. The main aim of the paper is to implement a Wireless Robot which can be controlled through PC using Ride and Flash magic interface and navigates around the disastrous area and tries to find the humans who need help. The Robot can detect the live human based on the IR radiation emerging from the humans. It is provided with a Proximity IR sensor for detecting live humans and for obstacle avoidance the robot is equipped with a robotic arm.

II. PROPOSED SYSTEM HARDWARE

The project proposes a mobile rescue robot that moves in the disaster prone area and helps in identifying the live people those are injured and performs rescue system operations. Hence due to the timely detection of victims precious life can be saved without the help of large number of rescue operators. The hardware system consists of a transmitter section and a receiver section. Figure below shows the block diagram of alive human detection robot.

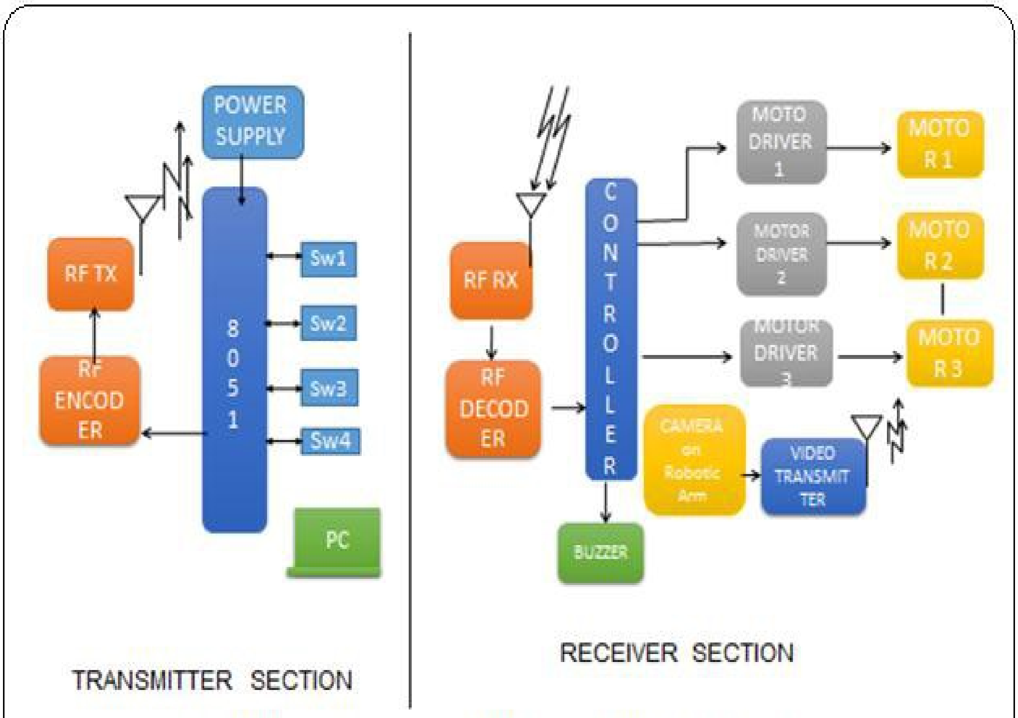


Fig. 1. Block Diagram Of Alive Human Detection System

II.1 Microcontroller

The microcontroller that is been used is the SST89E516RD controller. The microcontroller is used to gather the data from the sensor unit in real time and transfer the corresponding information data to the CPU of control room. It also receives commands from the CPU and transfers it to the robot unit for its movement. The microcontroller is the core of the surveillance robot [2]. It has an8K Bytes of In-System Programmable (ISP) Flash Memory. Operates at a range of 4.0V to 5.5V and has 256 x 8-bit Internal RAM.

II.2 Passive Infrared Sensor

A Passive Infra-Red sensor (PIR sensor) is an electronic device which measures infrared light radiating from objects in its field of view. Apparent motion is detected when an infrared source with one temperature, such as a human, passes in front of an infrared source with another temperature, such as a wall [1].

- *Design*

  Infrared radiation enters through the front of the sensor, known as the sensor face. At the core of a PIR is a solid state sensor or set of sensors, made from approximately 1/4 inches square of natural or artificial pyro electric materials, usually in the form of a thin film, out of gallium nitride (GaN), caesium nitrate (CsNO3), polyvinyl fluorides, derivatives of phenylpyrazine, and cobalt phthalocyanine. Lithium tantalate (LiTaO3) is a crystal exhibiting both piezoelectric and pyroelectric properties [1].
- *Features*
  a. Single bit output
  b. Jumper selects single or continuous trigger output
  c. Mode, 3-pin SIP header ready for breadboard or through whole Project.
  d. Small size makes it easy to conceal
  e. Compatible with BASIC Stamp, Propeller, and many other microcontrollers [1].

II.3 Camera module

The camera module consists of a web camera and it is mounted on the robot and the video signal is transmitted to the receiver at control room. The camera module will transmit the video coverage of the paths and thus helping in easier mapping of the path to be taken by the rescue team. For real time applications, camera of high range is to be used to get good clarity and good coverage of area. The function of camera also help the robot from getting stuck in a pit as the obstacles lying in path is foreseen and required action can be taken, thus improving the life of robot in the disaster area. Due to which we can observe the robot & we can see live vision [2].

II.4 Motor and motor driver

The robot driver unit is primarily concerned about the movement of the robot in x-axis and y-axis. The robot is of conveyor belt type as it helps to maneuver over debris and rugged terrain. Two DC motors of 200rpm will run the wheels of mobile rescue robot. When both the wheels are given with positive pulse edge, then robot moves in forward direction. When the supply is reversed mean both the wheels are given with negative pulse edge, then it goes in backward direction and similarly by varying the negative and positive edge, left and right turn can be achieve successfully. The selection of supply given to each motor, L293D IC is used. This will drive the robot to move in forward, reverse and turn left and right [2].

- **Features**
  a. Wide supply-voltage range: 4.5V to 36V.
  b. High-Noise-Immunity input.
  c. Peak output current 2 A per channel (1.2 A for L293D)

II.5 RF Module

An RF module (radio frequency module) is a small electronic device used to transmit and/or receive radio signals between two devices. In an embedded system like this it is desirable to communicate with another device wirelessly. This wireless communication may be accomplished through through radio frequency (RF) communication. For many applications the medium of choice is RF since it does not require line of sight. RF communications incorporate a transmitter and/or receiver.

- **RF transmitter**

  The encoder IC HT12E acts as a RF transmitter. HT12E is an 18 pin IC. It is capable of encoding 12 bits of information(4 data bits and 8 address bits). TE(transmission Enable) pin in the IC is responsible for transmission of data. Encoders are a series of CMOS LSIs for remote control system applications. They are capable of encoding information which consists of N address bits. Each address/data input can be set to one of the two logic states. The programmed addresses/data are transmitted together with the header bits via an RF or an infrared transmission medium upon receipt of a trigger signal. The HT12A additionally provides a 38 kHz carrier for infrared systems.

- **RF receiver**

  The decoder IC HT12D acts as a RF receiver. It is a 18 Pin DIP. Operating at a voltage of 2.4V~12V. It has low power and high noise immunity and low stand by current. It is capable of decoding 12 bits of information. It also converts the serial input into parallel outputs. These decoders are a series of CMOS LSIs for remote control system applications. For proper operation, a pair of encoder/decoder with the same number of addresses and data format should be chosen. The decoders receive serial addresses and data from a programmed series of encoders that are transmitted by a carrier using an RF or an IR transmission medium. These decoders are capable of decoding information that consists of N bits of address and data. Of this series, the HT12D is arranged to provide 8 address bits and 4 data bits.

III. SOFTWARE TOOLS

Software tools being used to interface the hardware system to software system are:

- RIDE
- FLASH Magic

III.1 RIDE (Raisonance 8051 Integrated Development Environment)

Ride is a full featured integrated development environment that provides seamless integration and easy access to all development tools. From editing to compiling, linking, debugging and back to start, with a simulator, ROM monitor or other debugging tool, RIDE conveniently manages all aspect of the embedded system development with a single user interface.

III.2 FLASH Magic

Flash Magic is a tool which is used to program hex code in EEPROM (Electrically Erasable Programmable Read Only Memory) of microcontroller. It supports the microcontroller of Philips and NXP. We can burn a hex code into those controllers which support ISP (in system programming) feature. If a device supports ISP then hex code can be easily burn into EEPROM of that device

IV. ADVANTAGES

- This system is an effective and a safe system to ensure that there are no humans left behind in a rescue operation.
- The system is safe even for the user because of the use of robotics and no manual work in field.[1]
- The design of this robot is simpler to understand.
- This system provides high reliability.
- They work efficiently in environment where it might be dangerous for humans.
- Precise positioning and repeatability of movement since good stepper motors have an accuracy of 3-5% of a step and this error is non-cumulative from one step to next.

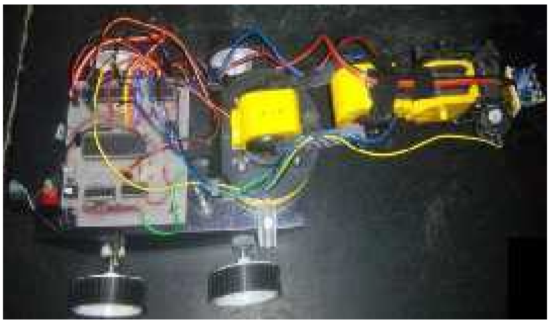
V. CONCLUSION

Hence many lives can be saved by using this autonomous vehicle during a disaster in a short duration which becomes time consuming and unaffected if done manually. The application of wireless sensor network will improve the saving of many lives by using mobile rescue robot in disaster prone area. In this paper we design an effective & safe system to ensure that there is no human left behind in rescue operation.

VI. HARDWARE OF ROBOT

VI.1 Transmitter

VI.2 Receiver



REFERENCES

[1] A.Sivasoundari, S.Kalaimani, M.Balamurugan: "Wireless Surveillance Robot with Motion Detection and Live Video Transmission"," *International Journal of Emerging Science and Engineering (IJESE)" ISSN: 2319-6378, Volume Issue-6 April2013.*

[2] Trupti B. Bhondve, Prof.R.Satyanarayan, Prof. Moresh Mukhedkar: "Mobile Rescue Robot for Human Body Detection in Rescue Operation of Disaster"," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering"*, Vol. 3, Issue 6, June 2014.

[3] Mr. S.P Vijayaragavan, Hardeep Pal Sharma,Guna sekar.C.H, S.Adithya Kumar: "Live Human Detecting Robot for Earthquake Rescue Operation"," *International Journal of Business Intelligents" Vol 02, Issue 01, June 2013.*

Internet of things Based Smart Car Parking System

Mr. S. BALABASKER
Associate Professor,
Department of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Mr. R. RADHAKRISHNAN
Assistant Professor,
Department of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Abstract – The increase in the number of vehicles leads to problem in vehicles parking at an appropriate place mainly the car parking which leads to traffic congestion. This is due to the fact that the current car park facility is unable to cope up with the arrival of large number of vehicles on the road. To solve this problem we propose a new idea "Internet of Thing Based Smart Car Parking System" which helps users to find a free parking space with the help of IoT. Our project uses Infrared sensor, Arduino Uno, ESP8266-01 Wi-Fi Module and Cloud server, It also lessens human effort at the parking area such as in case of searching of free slots by the driver and calculating the payment for each vehicle using parking area. Smart Car Parking System enables continuous monitoring and managing of available parking space in real-time thereby reducing the environmental pollution.

Index Terms— **IoT, RFID, IR sensors, smart parking, slot allocation,**

I. INTRODUCTION

Internet of things (IOTs) is a recent topic that plays an important role in our daily lives. IOT reduces human labor, effort, time and errors due to human negligence. With the development of modern technology, smart phones have become a necessity for every person on this planet. A smart parking system helps to monitor vehicle parking. It helps to manage parking collision among vehicles when they are parking at the same time that means it helps in synchronized parking. In IOT objects are connected to each other and exchange information from internet. Our IOT based smart parking organized the parking lot. It helps user to find a free space in parking slot. It saves user's time as well as their fuel. It helps nowadays to obtain parking spaces in metropolitan area which is very crucial. People waste money and fuel in searching for parking lot. Smart parking system gives information about parking spaces. An infrared (IR) sensor is used at each slot in parking; it tells the space availability. The information about the free or used slot sends over web page through IOT. Furthermore, we have other IOT platform like home automation, heart monitoring, any physical thing that is connected and exchanging information from internet. At present, Cisco is working very hard on IOT and probably up to year 2020 every appliance will be controlled by internet. Due to continue the growth of vehicle, it is difficult to find a parking place in a short amount of time and also it wasted a lot of fuel in searching an empty parking place. Hence, to overcome from this serious problem, we are implementing an automated parking where it can tell to user that parking space is available or not for his car. If slot is empty, they can go otherwise need search a new place instead of go and search for parking. In metropolitan area, smart car parking system becomes major point with rise numbers of vehicles. Normally, it takes more than 10 minutes to find parking space. This increases wastage of fuel, time and money. To control these limitations smart parking system using IOT based mobile application is proposed. It used global system for mobile communication/general packet radio service technology to overcome these limitations [7,8]. Anisotropic magneto-resistive sensors are used to obtain correct availability of parking slot (Fig. 1).

II. LITERATURE REVIEW

Paper [1,6] proposed a new algorithm for planning in real-time parking. The parking scheduling is converted into an off-line problem. The offline problem is described as a linear problem. The linear problem was solved using an algorithm. Finally, experimental simulations were done. However, this paper does not deal with the guiding of vehicles. Paper [2] proposes a solution for parking lot based on wireless sensor network and radio-frequency identification (RFID). The paper [2] however does not deal with a large scale parking lot. Paper [3] has proposed a parking system based on ZigBee network. Here, a web service is used to collect information about the parking space. Our approach is based on 8051 type microcontroller that is Arduino microcontroller, Arduino runs with Arduino IDE application that should be installed in system. We do simple embedded C code in microcontroller and directly put it into the Arduino system. We do simple embedded C code in microcontroller and directly put it into the Arduino microcontroller. Hence, it works according to code system keeps track of number of cars entered in parking building. The counting will be display using liquid crystal display board and IR sensor that sense the cars standing in front of parking gate.

III. PROPOSED SYSTEM

The proposed system is based on IOT. The parking lots are monitored using internet. The user can log on to the parking application and determine the free slot. In our paper, we determine the car parking lot that is nearest to the user. In case the parking lot is full then the system will also guide the user to the next nearest car park. The system architecture is described in Figure. 1. The system architecture is based on Arduino Uno microcontroller board, IR sensor, ESP8266 wifi module and Web server.

3.1 Block Diagram

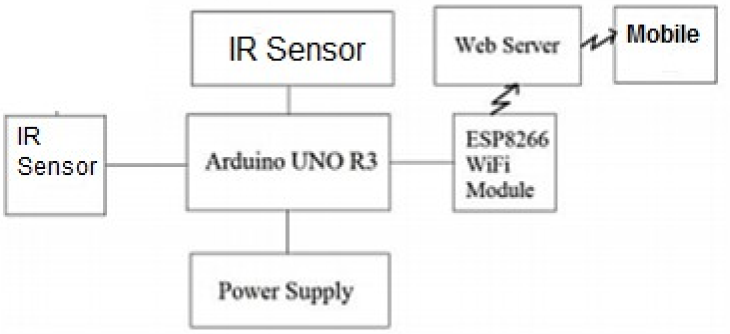


Figure 1. Block diagram of proposed system

3.2 Arduino UNO R3

The Arduino Uno is a microcontroller board based on the ATmega328 (datasheet). It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started.

The Uno differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features the Atmega16U2 (Atmega8U2 up to version R2) programmed as a USB-to-serial converter. Revision 2 of the Uno board has a resistor pulling the 8U2 HWB line to ground, making it easier to put into DFU mode.

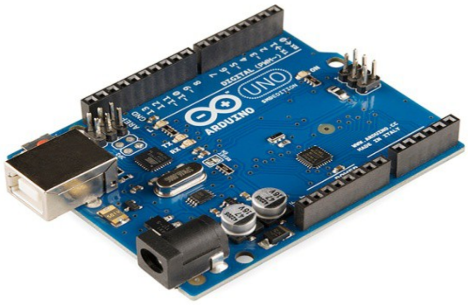


Figure 2. Arduino Uno R3

3.3 ESP8266-01 WiFi Module

ESP8266 offers a complete and self-contained Wi-Fi networking solution, allowing it to either host the application or to offload all Wi-Fi networking functions from another application processor. When ESP8266 hosts the application, and when it is the only application processor in the device, it is able to boot up directly from an external flash. It has integrated cache to improve the performance of the system in such applications, and to minimize the memory requirements. Alternately, serving as a Wi-Fi adapter, wireless internet access can be added to any microcontroller-based design with simple connectivity through UART interface .

Figure 3. ESP8266-01 WiFi Module

3.4 Android Studio

Android Studio is the official IDE for Android app development, based on IntelliJ IDEA. Android Studio offers even more features that enhance your productivity when building Android apps, such as:

- ✓ A flexible Gradle-based build system
- ✓ Build variants and multiple APK file generation
- ✓ Code templates to help you build common app features
- ✓ A rich layout editor with support for drag and drop theme editing

3.5 IR Sensor

An IR sensor is an electronic device that emits to sense some aspects of the surroundings. An IR sensor can measure the heat of an object as well as detects the motion. These types of sensors measure only IR radiation rather than emitting it, that is called as a passive IR sensor

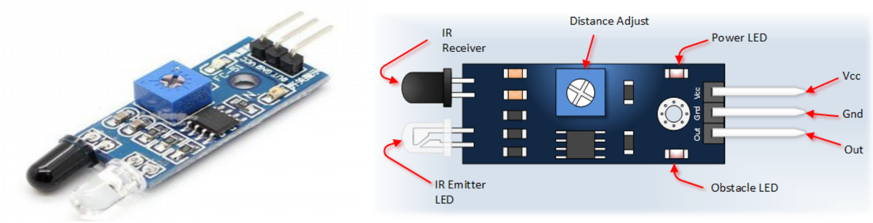


Figure 4. IR sensor & its specifications

3.6 Car parking system using cloud server

Cloud storage is a cloud computing model, in which data is stored on remote servers accessed from the internet, or “cloud” [9]. It is maintained, operated and managed by a cloud storage service provider on storage servers that are built on virtualization techniques. For some computer owners, finding enough storage space to hold all the data they've acquired is a real challenge. Some people invest in larger hard drives. Others prefer external storage devices like thumb drives or compact discs. Desperate computer owners might delete entire folders worth of old files to make space for new information. However, some are choosing to rely on a growing trend: Cloud storage.

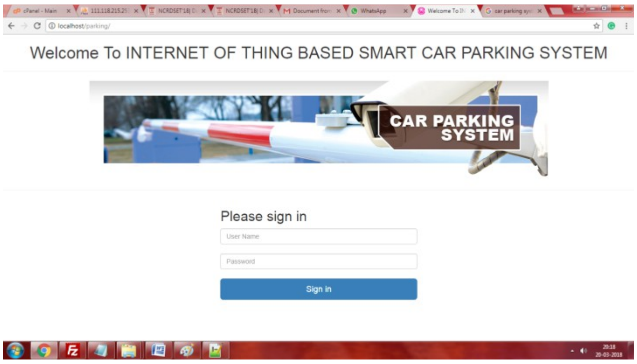
3.7 Guiding system to the nearest car park

In this paper, we find the nearest parking lot by considering the set of parking lots as a network [10]. Each node in the network is the parking lot. The RFID detects if the parking lot is full or empty. If it is empty, then the status is set as counter + 1 in the status table. The status table has the list of direct neighboring nodes and their distances from the current node. It also maintains the counter for vacancy in each neighboring car park. The distances are sorted in ascending order for all the neighboring parking lots with counter >1. The parking lot with the minimum distance and counter >1 is selected for booking. Once the parking lot is booked the counter of that parking lot is decreased by one. Whenever there are changes in the counter, it is updated in the server (Fig. 6).

IV.RESULT AND DISCUSSION

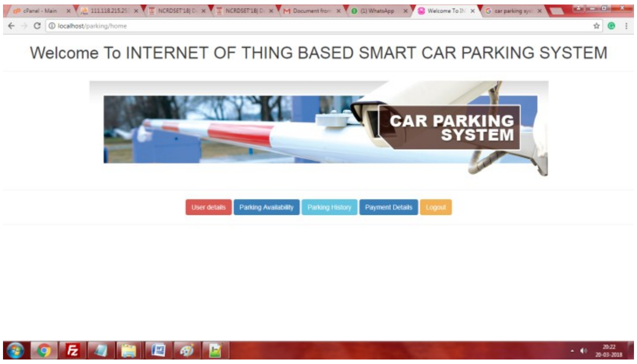
Arduino with the WIFI Shied for PC configuration of the physical address is mandatory. For Wifi, IP address is user defined if both IP address match. Hence, our hardware module will interact with PC. So next time a user can login or register with his authorized ID and password. Here are some login snapshots. So, a user can check for available space in the parking slot. Here, we have some snapshots of IOT based car parking. The concept is to improve making the car parking easy, workable; therefore, we developed smart car parking system (Fig. 5 to 9).

4.1 SOFTWARE OUTPUT



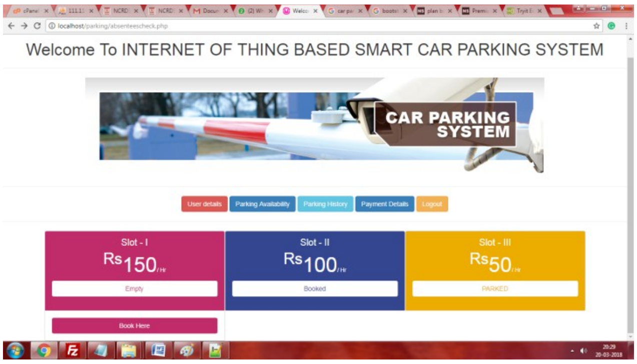
Welcome To INTERNET OF THING BASED SMART CAR PARKING SYSTEM

Figure 5. Login Page



Welcome To INTERNET OF THING BASED SMART CAR PARKING SYSTEM

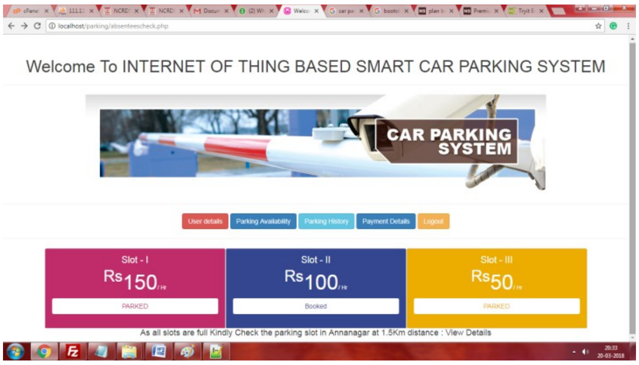
Figure 6. Home Screen



Welcome To INTERNET OF THING BASED SMART CAR PARKING SYSTEM

Slot - I	Slot - II	Slot - III
Rs150/Hr	Rs100/Hr	Rs50/Hr
Empty	Booked	PARKED
Book Here		

Figure 7. Availability in First Parking Area



Welcome To INTERNET OF THING BASED SMART CAR PARKING SYSTEM

Slot - I	Slot - II	Slot - III
Rs150/Hr	Rs100/Hr	Rs50/Hr
PARKED	Booked	PARKED

As all slots are full Kindly Check the parking slot in Annanagar at 1.5Km distance : View Details

Figure 8. If Slots are Full shows the nearest Parking Slot

4.2 HARDWARE OUTPUT

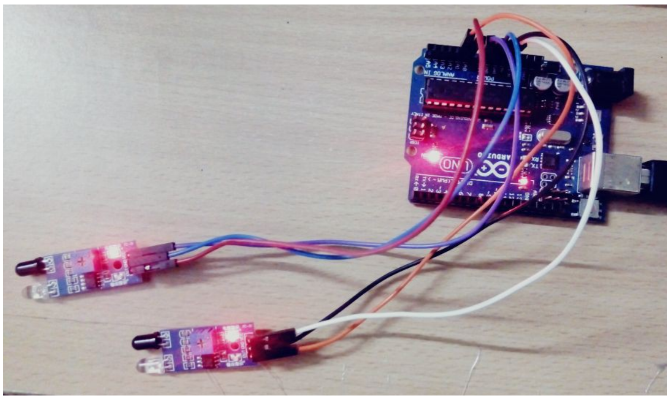


Figure 8. Arduino Uno reading the IR sensor values

V. CONCLUSION

From the proposed IOT based car parking, any passenger can register and login with his appropriate user id and password and then check for space availability of parking IOT. If space is available there, he will be allowed to go inside the parking IOT. A user can login and check for free space from anywhere which is the objective of car parking system using IOT. By using IOT, we can access information using internet. Nowadays, every person having a smart mobile phone uses internet. Hence, smart car parking system provides facility to book place for parking and it provides facility for user to pay fee online. By using user ID we can detect and identify owner name, address and so on. Smart parking system it is used for minimizing manpower as well as fuel. The enhancement of the paper is to consider the traffic in the path of various car parks.

VI. REFERENCES

1. Geng Y, Cassandras CG. A new smart parking system based on optimal resource allocation and reservations. In: Proceeding of 14th International IEEE Conference on Intelligent Transportation Systems; 2011. p. 979-84.
2. Geng Y, Cassandras CG. New smart parking system based on resource allocation and reservations. IEEE trans Intell Transp Syst 2013;14(3):1129-39.
3. Shiyao C, Ming W, Chen L, Na R. The research and implement of the intelligent parking reservation management system based on ZigBee technology. Proceeding 6th International Conference on Mechatronics and Automation Technology Mechatronics Automation. (ICMTMA); 2014. p. 741-4.
4. Sen S, Chakrabarty S, Toshniwal R, Bhaumik A. Design of intelligent voice controlled home automation system. Int J Comput Appl 2015;121(15):39-42.
5. Gandhi BM, Rao K. Aprototype for IOT based car parking management system for smart cities. Indian J Sci Technol 2016;9(17). DOI: 10.17485/ijst/2016/v9i17/92973.
6. Vishwanath Y, Kuchalli AD, Rakshit D. Survey paper on smart parking system based on internet of things. Int J Recent Trends Eng Res 2016;2(3):156-60.
7. He W, Yan G, Xu LD. Developing vehicular data cloud services in the IOT environment. IEEE Trans Ind Inform 2014;10(2):1587-95.
8. Basavaraju SR. Automatic smart parking system using internet of things (IOT). Int J Sci Res Publ 2015;5(12):629-32.
9. Pham TN, Tsai MF, Nguyen DB, Dow CR, Deng DJ. A cloud-based smart-parking system based on internet-of-things technologies. IEEE Access 2015;3:1581-91.

10. Ichake VD, Shitole PD, Momin M, Thakare KS. Smart car parking system based on IOT concept. Int J Eng Sci Invent 2016;5(3):48-54.

FFT Approaches to Analyze the Periodic Characteristics of ECG Waveform

Mrs. D. Umamaheswari,
Associate Professor,
Department of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Mrs. M. Mary Amala Jenni,
Assistant Professor,
Department Of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Mrs. M. Vaidehi
Professor,
Department Of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Abstract:

Digital Signal Processing (DSP) Applications have gained great popularity in the study of Bio-Medical Signal Processing .DSP can be used as a tool in the era of Bio-Medical Engineering and it is used to study the continuous rhythmic periodic waveform of ECG and finding out abnormalities present in the function of the heart.DSP solves this task with great accuracy and less complexity. According to available medical research report it has been given to understand the arrhythmias caused due to cardiac abnormalities. In this project we are going to present FFT approaches to analyze the periodic characteristics of ECG waveform and design spectrum of Angina Pectoris of ECG for identifying cardiac abnormalities.

1. INTRODUCTION

Application of signal processing methods, such as filtering, Discrete Fourier Transform (DFT), Fast Fourier transform (FFT) to biomedical problems, such as the analysis of cardiac signals (ECG/EKG).

The signal processing in digital is what we are considering to implement to our ECG signals as an extra function after we finish the basic objective of the project, which is only to design, simulate, fabricate, test, and demonstrate an ECG demonstration board in analog.

1.1 DSP Techniques:

Digital signal processing and analog signal processing are subfields of signal processing. DSP applications include audio and speech signal processing, sonar, radar and other sensor array processing, spectral estimation, statistical signal processing, digital statistical signal processing, digital image processing, signal processing for telecommunications, control of systems, biomedical engineering, seismic data processing, among others, Digital signal processing can involve linear or nonlinear operations. Nonlinear signal processing is closely related to nonlinear system identification and can be implemented in the time, frequency, and spatial-temporal domains. The application of digital computation to signal processing allows for many advantages over analog processing in many applications, such as error detection and correction in transmission as well as data compression. DSP is applicable to both streaming data and static (stored) data.

2. BLOCK DIAGRAM

2.1 Normal ECG waveform:

The fundamental component to electrocardiograph is the Instrumentation amplifier, which is responsible for taking the voltage difference between leads (see below) and amplifying the signal. ECG voltages measured across the body are on the order of hundreds of micro volts up to 1 milli volt (the small square on a standard ECG is 100 micro volts). This low voltage necessitates a low noise circuit and instrumentation amplifiers are key.

Early electrocardiographs were constructed with analog electronics and the signal could drive a motor to print the signal on paper. Today, electrocardiographs use analog-to-digital converters to convert to a digital signal that can then be manipulated with digital electronics. This permits digital recording of ECGs and use on computers.

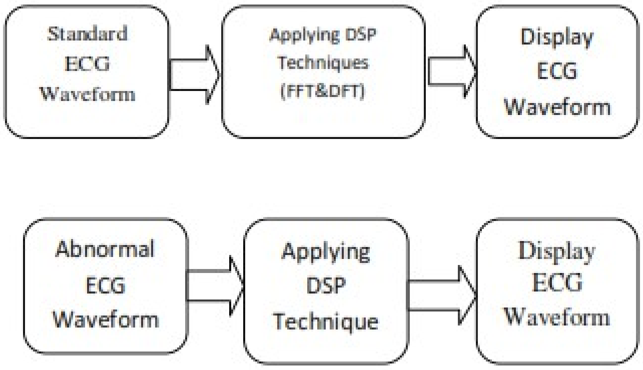


Fig.1. Block diagram of techniques applied to ECG waveform.

Physiological data are displayed continuously on a CRT, LED or LCD screen as data channels along the time axis. They may be accompanied by numerical readouts of computed parameters on the original data, such as maximum, minimum and average values, pulse and respiratory

Frequencies, and so on. Besides the tracings of physiological parameters along time (X axis), digital medical displays have automated numeric readouts of the peak and/or average parameters displayed on the screen. Contraction of the heart muscle occurs in response to electrical depolarisation the rapid spread of electrical activity throughout the myocardium which is facilitated by specialized conduction tissue. This process normally begins with spontaneous depolarisation of cells in the sinus node, situated in the right atrium (RA), then proceeds quickly through the atria to the atrioventricular node, and then down the bundle of His to the left and right bundle branches and into the ventricular myocardium.

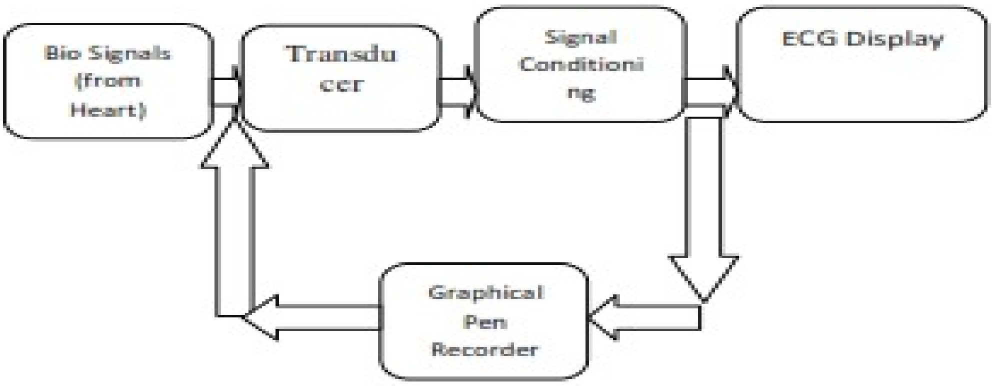


Figure: 2.2 Block diagram of ECG Implementation

2.2 Bio signals:

The term bio signal is often used to refer to bioelectrical signals, but it may refer to both lectrical and non-electrical signals. The usual understanding is to refer only to time-varying signals, although spatial parameter variations (e.g. the nucleotide sequence determining the genetic code) are sometimes subsumed as well. Electric bio signals such as EEG and ECG can be measured without electric contact with the skin. This can be applied for example for remote monitoring of brain waves and heart beat of patients who must not be touched, in particular patients with serious burns.

2.3 Transducer:

A transducer is a device that converts one form of energy to another. Usually a transducer converts a signal in one form of energy to a signal in another. Transducers are often employed at the boundaries of automation, measurement, and control systems. Electrical signals are converted to and from other physical quantities (energy, force, torque, light, motion, position, etc.). The process of converting one form of energy to another is known as transduction

2.4 Passive:

Passive sensors require an external power source to operate, which is called an excitation signal. The signal is modulated by the sensor to produce an output signal.

2.5 Active:

Active sensors generate electric signals in response to an external stimulus without the need of an additional energy source.

2.6 Sensors:

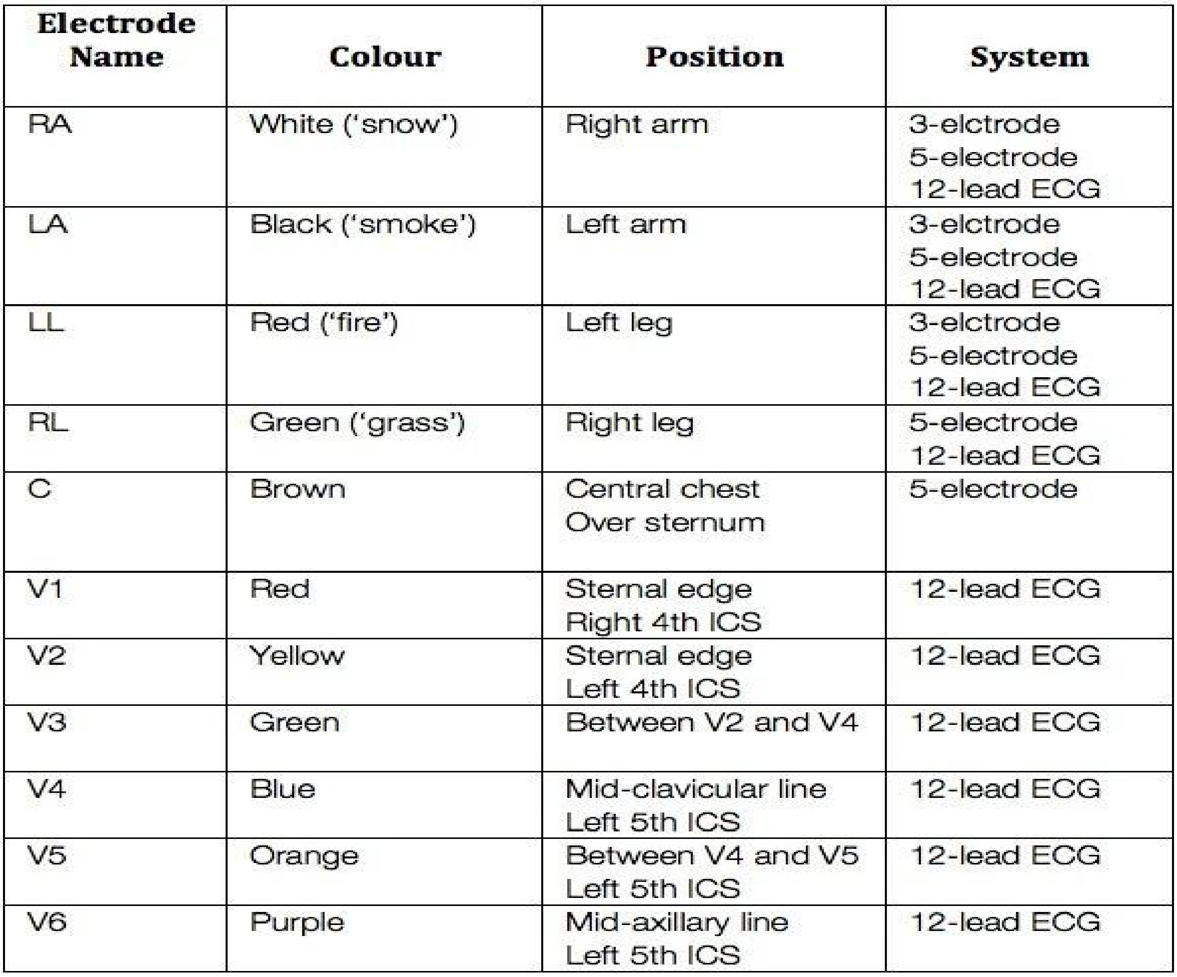
A sensor is a device that receives and responds to a signal or stimulus. Transducer is the other term that is sometimes interchangeably used instead of the term sensor, although there are subtle differences. A transducer is a term that can be used for the definition of many devices such as sensors, actuators, or transistors.

2.7 Actuators:

An actuator is a device that is responsible for moving or controlling a mechanism or system. It is operated by a source of energy, which can be mechanical force, electrical current, hydraulic fluid pressure, or pneumatic pressure, and converts that energy into motion. Graphic recorders are essentially measuring instruments that produce in real-time graphic representations of (biomedical) signals, in the form of a permanent document intended for visual inspection. Recorded data are thus fixed on a two-dimensional (2D) medium that can simply be called “paper”. Real-time paper recordings have the benefit of direct visual access to signal information, allow immediate examination (and re-examination) of trends (as long strips of paper can be used), present better graphic quality than most screens and can be used as a document for scientific evidence.

3. ELECTROCARDIOGRAM

An electrocardiograph with integrated display and keyboard on a wheeled cart an electrocardiograph is a machine that is used to perform electrocardiography, and produces the electrocardiogram. The first electrocardiographs are discussed above and are electrically primitive compared to today's machines. The fundamental component to electrocardiograph is the Instrumentation amplifier, which is responsible for taking the voltage difference between leads (see below) and amplifying the signal. ECG voltages measured across the body are on the order of hundreds of micro volts up to 1 milli volt (the small square on a standard ECG is 100 micro volts). Early electrocardiographs were constructed with analog electronics and the signal could drive a motor to print the signal on paper. Today, electrocardiographs use analog-to-digital converters to convert to a digital signal that can then be manipulated with digital electronics. This permits digital recording of ECGs and use on computers.



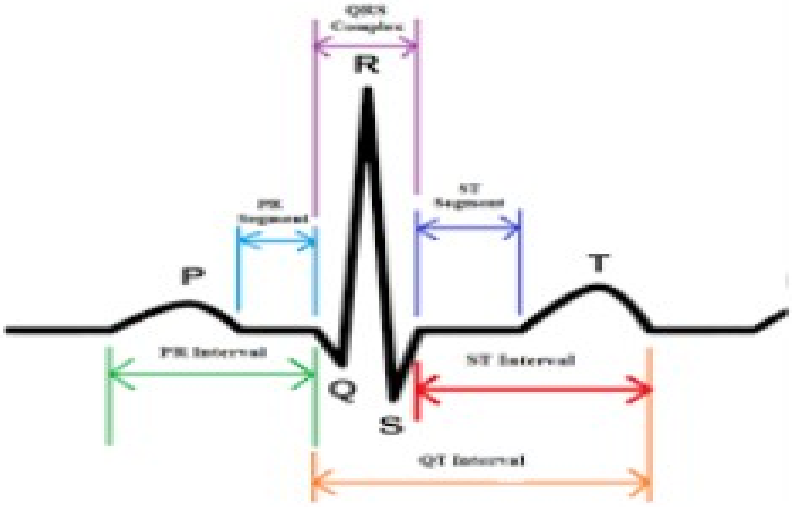
Electrode Name	Colour	Position	System
RA	White ('snow')	Right arm	3-elctrode 5-electrode 12-lead ECG
LA	Black ('smoke')	Left arm	3-elctrode 5-electrode 12-lead ECG
LL	Red ('fire')	Left leg	3-elctrode 5-electrode 12-lead ECG
RL	Green ('grass')	Right leg	5-electrode 12-lead ECG
C	Brown	Central chest Over sternum	5-electrode
V1	Red	Sternal edge Right 4th ICS	12-lead ECG
V2	Yellow	Sternal edge Left 4th ICS	12-lead ECG
V3	Green	Between V2 and V4	12-lead ECG
V4	Blue	Mid-clavicular line Left 5th ICS	12-lead ECG
V5	Orange	Between V4 and V5 Left 5th ICS	12-lead ECG
V6	Purple	Mid-axillary line Left 5th ICS	12-lead ECG

Table 1. ECG Electrodes

3.1 ECG Intervals:

- PR interval.
- PR segment.
- QRS complex.
- QT interval.
- ST segment.
- RR interval.
-

The PR interval begins at the onset of the P wave and ends at the onset of the QRS complex. This interval represents the time the impulse takes to reach the ventricles from the sinus node. It is termed the PR interval because the Q wave is frequently absent. Normal values lie between 0.12 and 0.20 seconds.



The PR segment begins at the endpoint of the P wave and ends at the onset of the QRS complex. It represents the duration of the conduction from the atrio ventricular node, down the bundle of His and through the bundle branches to the muscle. The QRS represents the duration of ventricular depolarisation. Normally all QRS complexes looks alike. They are still termed QRS complexes even if all three waves are not visible. The QT interval represents the duration from the depolarisation to the repolarisation of the ventricles. It begins at the onset of the QRS complex and ends at the endpoint of the T wave. The ST segment begins at the endpoint of the S wave and ends at the onset of the T wave. During the ST segment, the atrial cells are relaxed and the ventricles are contracted so electrical activity is not visible. The ST segment is normally isoelectric. The RR interval is the time measurement between the R wave of one heartbeat and the R wave of the preceding heart beat. RR intervals are normally regular, but may be irregular with sinus node disease and supra ventricular arrhythmias.

4. DIGITAL SIGNAL PROCESSING

Digital signal processing refers to various techniques for improving the accuracy and reliability of digital communications. The theory behind DSP is quite complex. Digital signal processing (DSP) is the use of digital processing, such as by computers, to perform a wide variety of signal processing operations. The signals processed in this manner are a sequence of numbers that represent samples of a continuous variable in a domain such Basically, DSP works by clarifying, or standardizing, the levels or states of a digital signal". as time, space, or frequency.

4.1 FFT:

An FFT computes the DFT and produces exactly the same result as evaluating the DFT definition directly; the most important difference is that an FFT is much faster. (In the presence of round-off error, many FFT algorithms are also much more accurate than evaluating the DFT definition directly, as discussed below.)

Let X_0, ..., X_{N-1} be complex numbers. The DFT is defined by the formula

$$\mathrm{X_K} = \sum_{n}^{N-1} Xn\ e^{-j2\pi kn/N} \qquad \mathrm{K=0,....,}$$

$$\mathrm{N\text{-}1.}$$

This series describes the distribution of power into frequency components composing that signal. According to Fourier analysis any physical signal can be decomposed into a number of discrete frequencies or a spectrum of frequencies over a continuous range. The statistical average of a certain signal or sort of signal (including noise) as analyzed in terms of its frequency content is called its spectrum.

The average power P of a signal over all time is therefore given by the following time average:

$$\mathrm{P}{=}\lim_{T\to\infty}\frac{1}{T}\int_{-T}^{T}|X(T)|\hat{}2\ \mathrm{dt}$$

5. MATLAB

MATLAB is a high performance language for technical computing. It integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notations.

MATLAB is an interactive system whose basic data element is an array that does not require dimensioning. This allows you to solve many technical computing problems, especially those with matrix and vector formulations, in a fraction of the time it would take to write a program in a scalar non interactive language such as C or FORTRAN.

6. RESULTS

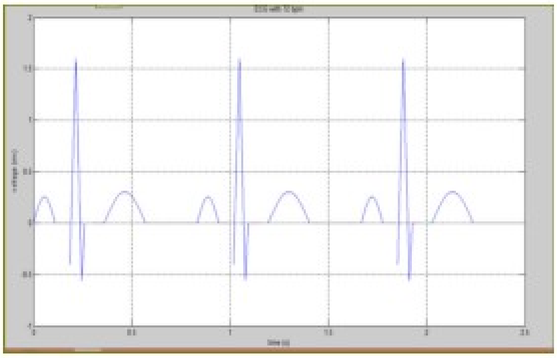


Figure 7.1: Normal ECG output waveform

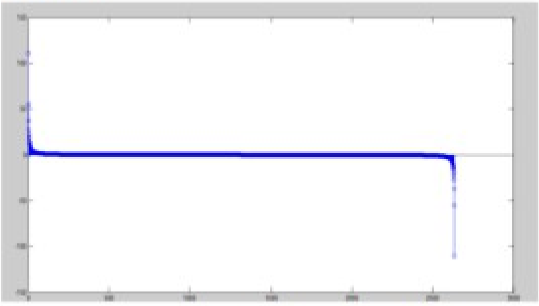


Figure7.2: Normal ECG FFT output

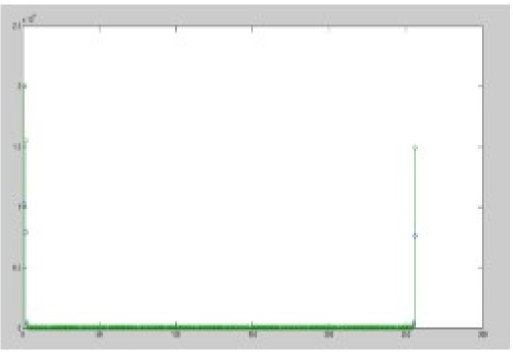


Figure 7.6 : Abnormal ECG –PSD output waveform

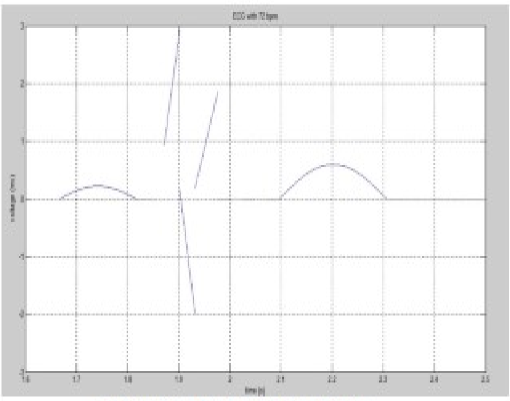


Figure 7.3: Abnormal ECG –Output waveform

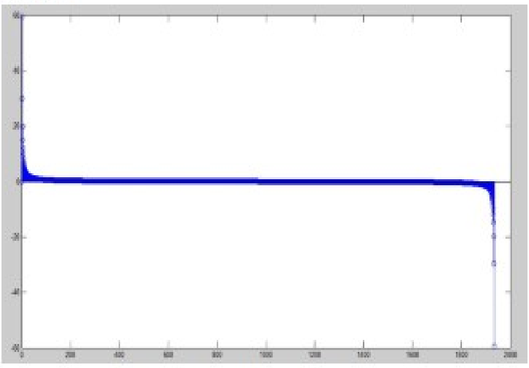


Figure 7.4: Abnormal ECG FFT output

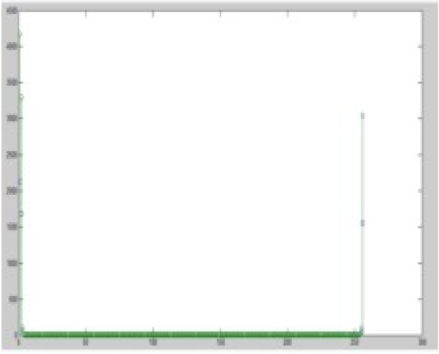


Figure 7.5 : Normal ECG –PSD output waveform

7. CONCLUSION

Hence we find DSP can be used as a tool in the era of Bio-Medical Engineering and it is used to study the continuous rhythmic periodic waveform of ECG and Digital Signal Processing (DSP) Applications are very useful in the study of finding out abnormalities present in the function of the heart. And we prove DSP solves this task with great accuracy and less complexity. In this project we are present DFT approaches to analyze the periodic characteristics of ECG waveform and we describe the spectrum of Angina Pectoris of ECG for identifying cardiac abnormalities.

REFERENCES

Walraven, G. (2011). Basic arrhythmias (7th ed.), pp. 1–11

"ECG- simplified. Aswini Kumar M.D." LifeHugger. Retrieved 11 February 2010.

Charles Van Loan, Computational Frameworks for the Fast Fourier Transform (SIAM, 1992).

Strang, Gilbert (May–June 1994). "Wavelets". American Scientist. 82 (3): 253. JSTOR 29775194

James W. Cooley, "The Re-Discovery of the Fast Fourier Transform Algorithm",ReferencesMikrochimica Acta [Wien],1987, III, 33–45.

Percival, Donald B.; Walden, Andrew T. (1992). Spectral Analysis for Physical Applications. Cambridge University Press.

Lerga, Jonatan. "Overview of Signal Instantaneous Frequency Estimation Methods".

Gilat, Amos (2004). MATLAB: An Introduction with Applications 2nd Edition. John Wiley & Sons. ISBN 978-0-471-69420-5.

Quarteroni, Alfio; Saleri, Fausto (2006). Scientific Computing with MATLAB and Octave. Springer. ISBN 978-3-540-32612-0

Energy efficient path detection and traffic reduction using EDAL protocol in WSN

[1]Antoni Raj R, [2] Arun Raj G S, [3] Balaji R
[1,2,3,4] UG students,
Department of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Mrs. D. Umamaheswari,
Associate Professor,
Department of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Mrs. M. Vaidehi,
Professor,
Department of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Abstract-The Wireless Sensor Networks (WSNs) have emerged as a new category of networking systems with limited computing, communication, and storage resources. In many sensing applications source nodes deliver packets to sink nodes via multiple hops, leading to the problem on how to find routes that enable all packets to be delivered in required time frames, while simultaneously taking into account factors such as energy efficiency and load balancing. To solve this problem one data collection protocol is developed called EDAL, which stands for Energy-efficient Delay-aware Lifetime-balancing data collection. Methods used are centralized heuristic and ant colony gossiping to find best energy efficient path. CAS (Cooperation-Aware Scheme) is used to reduce the traffic in the network.

Index Terms— Ant colony gossiping, Centralized heuristic

I. INTRODUCTION

Wireless Sensor Network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. A WSN consists of few hundreds to thousands of sensor nodes. The sensor node equipment includes a radio transceiver along with an antenna, a microcontroller, an interfacing electronic circuit, and an energy source, usually a battery. The size of the sensor nodes can also range from the size of a shoe box to as small as the size of a grain of dust.

The main constraint of sensor nodes is their very low finite battery energy, which limits the lifetime and the quality of the network . For that reason, the protocols running on sensor networks must consume the resources of the nodes efficiently in order to achieve a longer network lifetime.Finding best energy efficient path using Centralized Heuristic and Ant colony Optimization. Reducing the network traffic using Cooperative Aware Scheme in Wireless sensor network.

This paper develops EDAL, an *E*nergy- efficient *D*elay-*A*ware *L*ifetime-balancing data collection protocol. Specifically, EDAL is formulated by treating energy cost in transmitting packets in WSNs in a similar way as delivery cost of goods in OVR and by treating packet latencies similar to delivery deadlines. So introduce both centralized heuristic based on tabu search and a distributed heuristic based on ant colony gossiping, to obtain approximate solutions. Our algorithm designs also take into account load balancing of individual nodes to maximize the system lifetime.

II. EXISTING SYSTEM

The vehicle routing problem (VRP) is a well- known NP-hard problem in operational research. VRP finds routes between a depot and customers with given demands so that the transportation cost is minimized with the involvement of the minimal number of vehicles, while satisfying capacity constraints. With additional constraints, VRP can be further extended to solve different problems, where one of the most important is the vehicle routing problem with time windows (VRPTW). This problem occurs frequently in the distribution of goods and services, where an unlimited number of identical vehicles with predefined capacity serve a set of customers with demands of different time intervals (time windows). VRPTW tries to minimize the total transportation cost through the minimum number of vehicles, without violating any timing constraints.

Once routes have been found using EDAL, further refine the data collection efficiency through an emerging technique calledCompressive Sensing. CS is a technique through which data are compressed during their transmission to a given destination by exploiting the fact that most sensors may not always have valid data to report when they sample the environment , especially for nodes deployed in stable environments with rare and infrequent events to be detected.

A new data aggregation technique derived from CS to minimize the total energy consumption through joint routing and compressed aggregation Compressive sensing and particle swarm optimization algorithms to build up data aggregation trees and decrease communication rate. These two methods are different from EDAL in that they require all nodes to contribute sensing data during the data collection phase.

III. PROPOSED SYSTEM

Key motivation for this work stems from the insight that recent research efforts on open vehicle routing (OVR) problems are usually based on similar assumptions and constraints compared to sensor networks. Specifically, in OVR research on goods transportation, the objective is to spread the goods to customers in finite time with the minimal amount of transportation cost.

One may wonder, naturally, if treating packet delays as delivery time of goods, and energy cost as delivery cost of goods, it may be possible to exploit research results in one domain to stimulate the other.

Motivated by this observation EDAL, an Energy- efficient Delay-Aware Lifetime-balancing Protocol is developed. Specifically, EDAL is formulated by treating energy cost in transmitting packets in WSNs in a similar way as delivery cost of goods in OVR and by treating packet latencies similar to delivery deadlines.

To reduce its computational overhead, introduce both a centralized metaheuristic based on tabu search and a distributed heuristic based on ant colony gossiping, to obtain approximate solutions. This also takes into account load balancing of individual nodes to maximize the system lifetime.

On the other hand, the proposed CAS is a cooperative strong nodemechanism in which a threshold is preset in order to determine whether the node traffic is over or not. The privilege of corresponding sensor nodes is upgraded when the load exceeds the threshold. Therefore, the sensor node can command its child nodes to change the transmission path for distributing the traffic effectively. Moreover, once the traffic is over the overall network flow threshold, it is necessary to add the other new sensor nodes into the network for relieving the traffic.

IV. SYSTEM MODEL

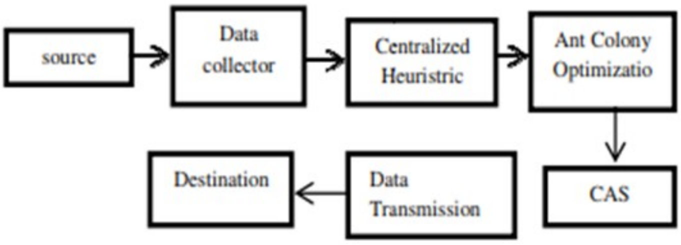


Figure 4.1 System Architecture

In Figure 4.1 the system architecture contains 4 main parts, i.e., Configuration Manager, Centralized Heuristic, Ant Colony Optimization and Cooperative Aware Scheme. First create a Wireless Sensor Network .A Wireless Sensor Network consists of many number of sensor nodes. From the large number of sensor node, select a source node so as to transmit data to the destination node. Each node in the sensor network performs status gossiping. Based on centralized heuristic, route to reach the destination node will be constructed. The status gossip helps to store the details about nodes in the database. For example remaining energy level of nodes, path to reach the nodes are all stored. Sensor network depends on lifetime of the sensor node in the Wireless Sensor Networks. CAS is used when the network flow exceeds the capacity to reduce congestion.

4.1 Data Collector

This is used to collect the date from the network. This creates the sensor nodes in the wireless sensor network. This data collector performs the process of monitoring and controlling the network devices to find where the nodes are located. This module organizes and maintain the details about all components of the network. This component collects the packets from the networks, which are in-turn specified by the user and transfer it to the destination. This also identifies the source and destination to transfer the data.

4.2 Centralized Heuristic

The centralized heuristic algorithm consists of two phases one is route construction, which finds an initial feasible route solution, and route optimization which improves the initial results using the tabu search optimization technique. In the route construction phase of this algorithm, we present a heuristic algorithm based on the Revised Push Forward Insertion

Heuristic (RPFIH) method. RPFIH repeatedly selects the customer with the lowest additional insertion cost as the next node, until all customers are connected.

Finally, RPFIH generates a set of found routes as the final output. Next optimize the initial solution using tabu search. Tabu search is a popular memory-based search strategy for guiding search beyond locally optimal points. Specifically, tabu search keeps the following data structures. One is tabu move list which is a queue with fixed size to keep the recent moves, so that problems such as repetition and cycling can be avoided. Other one is candidate list that stores the best solutions found so far by the search process, ranked by their total route cost.

4.3 Ant Colony Optimization

In Ant Colony Optimization, each node sends forward ants spreading its current status, including its remaining energy level, toward its neighbor nodes within H hops. Meanwhile, the status data of nearby nodes is collected by each source node with the received backward ants. The status Gossips used to store the status information of various nodes.

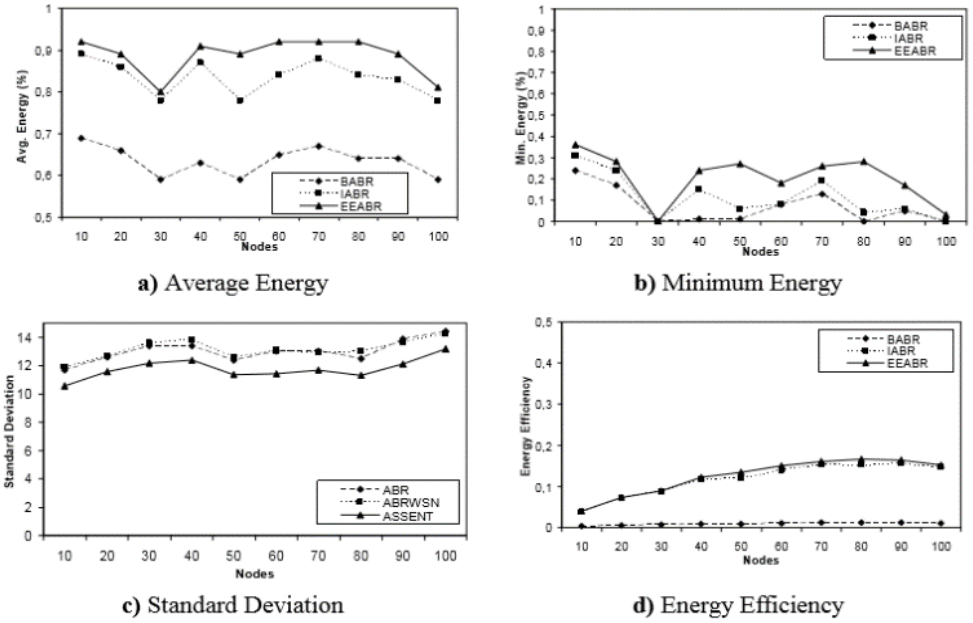
In the status gossiping phase, each source node sends forward ants spreading its current status, including its remaining energy level, toward its neighbor source nodes within some hops. Meanwhile, the status data of nearby nodes is collected by each source node with the received backward ants. During the gossip phase, the ants are forwarded with a modified geographic forwarding routing protocol, which chooses the node with the maximum remaining energy while making geographical progress toward the destination as the next hop.

Once a node collects status information of all its nearby sources, it enters the route construction phase and runs RPFIH distributed based on collected nearby neighbor status and the estimation of node status outside the immediate neighborhood. As all nodes start with a fixed amount of energy according to the node type, the source node can accurately estimate the status of nearby nodes. In that case, the minimal weight path from a source node to a nearby source node can be calculated with the currently held information.

4.4 Cooperative Aware Scheme

In CAS scheme, the buffer loading is applied to detect the outcome of congestion problems. When the buffer loading is higher than the preset threshold, there are impending congestion problems, thereby, the operating node mode is going to be switched into the strong node mode for reducing the network traffic. The transmission path and the node traffic of a child node is changing and observing, respectively, when in the strong node mode. By this object reconstruction with feature distribution scheme, efficient processing has to be done on the images received from nodes to reconstruct the image and respond to user query. Object matching methods form the foundation of many state- of-the-art algorithms. Therefore, this feature distribution scheme can be directly applied to several state-of- the-art matching methods with little or no adaptation. The future challenge lies in mapping state-of-the-art matching and reconstruction methods to such a distributed framework. The reconstructed scenes can be converted into a video file format to be displayed as a video, when the user submits the query. This work can be brought into real time by implementing the code on the server side/mobile phone and communicate with several nodes to collect images/objects. This work can be tested in real time with user query results. The algorithm of CAS mainly designed to avoid packets dropped by nodes due to high traffic loading. When a node is in danger of being overloading, part of the traffic is distributed to other nodes before the occurrence of the congestion problem.

V.RESULT



a) Average Energy

b) Minimum Energy

c) Standard Deviation

d) Energy Efficiency

VI. CONCLUSION

An Energy efficient Delay Aware Lifetime balancing EDAL protocol was proposed in wireless sensor networks which are promoted by flourishing techniques developed for open vehicle routing problems with time deadlines. The proposed system EDAL solves the problem of high energy consumption in sensor networks by balancing the loads in nodes. The centralized heuristic algorithm generate routes that connect all nodes with minimal total path cost, under the constraints of packet delay requirements. Ant colony optimization is used to find the best path to transfer the data. The lifetime of the deployed sensor network is also balanced by assigning weights to links. Here high energy nodes are chosen to balance the load which in turn increases the lifetime of wireless sensor network. Thus traffic in the network also reduced by finding alternate route when congestion occurs which in turn reduces delay.

REFERENCES

[1] Anuba Merlyn “Energy Efficient Routing (EER) For Reducing Congestion and Time Delay in Wireless Sensor Network”International Journal of Computer Networks and Applications Volume 1, Issue 1, November - December (2014)

[2] Chen G, Guo T.D, Yang W.G. and Zhao T. (2006), „An improved ant based routing protocol in wireless sensor networks", Proc. CollaborateCom, pp. 17.

Identification of Car Parking Slot availability Using IOT

[1]M.Aarthi, [2]J.Arunadevi, [3]V.Jayasri, [4]R.Joyrafalin,
[1,2,3,4] Department of Electronics and Communication Engineering
St. Anne's College of Engineering and Technology, Anguchettypalayam, Panruti.

S.Balabasker
Associate Professor,
Department Of Electronics And Communication Engineering
St. Anne's College Of Engineering Technology, Anguchettypalayam, Panruti.
mailto:balabasker.s@gmail.com, mobile:9944374993

Abstract:

This paper focus on multilevel car parking system A using internet of things by sending the status of the parking slot to the internet.IR sensor and Arduino in combination with usage of internet of things by sending the information to the mobile phone, laptops , LCD screens ,etc..The implementation of multilevel car parking system helps us for parking more number of cars with minimum space. Our proposed system deals with information about parking slot availability using IOT. Authentication card will provided for the each car so that the authorized can access the parking system .The advantage of multilevel parking are to solve the parking issue in the urban area and also provide the security to a car. It can be used in highly populated areas such as hospitals, schools, colleges, shopping mall, cinema halls, etc.,

Keywords: ***Internet of Things (IoT), Autonomous Car Parking, Arduino, ESP8266 Wi-Fi Module, IR Sensors, Servo motor.***

I. INTRODUCTION

In this age of technology, we are working in a way to reduce our effort in every possible way and the introduction of the Arduino and IoT platforms have further broadened the scope of this possibility in our everyday lives. One of the major problems that we are facing in today's over-populated society is finding available parking spots in various public places like hospitals, office shopping malls, cinema halls, courts, schools and colleges.

The statistics show that approximately 20% of all the congestion in the city is caused by frustrated drivers driving around the block searching for parking spaces.

II. PREVIOUS WORK

Various parking sensors are already installed in some of the public spaces in developed countries which use infrared sensors (hereinafter called as IR Sensors) to detect the presence of a car in a particular spot.

The motivation that drives the result is the pursuit of an alternative solution for the problem that is instead of using IR Sensors, it would be more efficient to switch to Ultrasonic Sensor which is not affected by variations in the light intensity in a particular environment. Also, instead of using the Ethernet shield or connecting it through LAN cable, a Wi-Fi module (ESP8266) is used. Thus, reducing the cost of cable, increasing the efficiency and making it more feasible to get implemented.

2.1 Using hardware: Indicators (in this case, two bulbs: 1 red and 1 green) are placed outside the parking slot, red bulb indicating an occupied parking space while the green bulb which indicates an empty space. This is done so that during the night time the driver can see from a distance that is the slot is empty or occupied.

2.2

2.3 Software (IoT): Before entering the place, the driver can check through the Internet/Mobile App that which slot or which area is empty and can directly go to that area and park his car, without anyone's help or the Security personnel in the public parking areas or the malls can check the spots in their systems and can direct the incoming cars to the particular locations.

III. ENTRY: When the user reaches parking gate, he will punch the RFID card on RFID reader. Reader will read the tag and sends its information to Arduino and check whether ID is authorized or not. If it is authorized, then signal will be send to electric motor to open gate. Once the car gets entry, gate will be closed and once parked free parking space counter will be reduced by 1. Immediately notification will be send to user's mobile that car has been parked at this place. If the user is authorized and free parking space is not available, then Arduino will send signal to display that parking is not free and hence gate will not opened. If the user is unauthorized then again Arduino will send it to display to show that UNAUTHORIZED and will not allow to open gate.

IV. EXIT: Car moves from the parking space, IR sensor sense it and increases free parking space by 1. User punch its card to RFID reader, If he is authorized the Arduino will send signal to motor to open gate. If he is not authorized then gate will not be opened and he will not be allowed to go out and if he is fraud then easily he can be caught. The entry and exit loop is shown in Figure 1. The car enters from entry point. When the car is parked on parking slot, IR sensor at this place sense the car and hence it reduces available parking slot counter by 1 and display on LED.

V. OVERVIEW:

5.1 AIM:

- To make it convenient for the driver to check whether the slot is empty or occupied.
- To develop a autonomous car parking system using Arduino and IOT platform and display the output.
- Reducing parking space in highly congested multi level parking system.
- It can be used in finding free parking spot in various public place.
-

5.2 COMPONENT USED:

- An arduino Uno board or ATMEGA328 chip to program the hard ware.
- IR sensor used to detect the object in precise output.
- Servo motor can used to open the gate
- A Wi-Fi module(ESP 8266) is used to send the IR sensor data through the internet

VI(a) . BLOCK DIAGRAMFOR TRANSMITTER

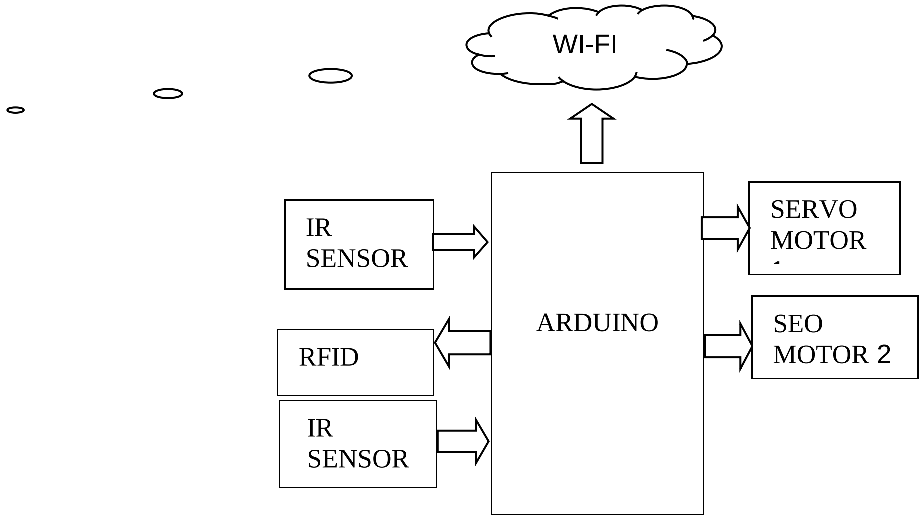


fig1. Block diagram of Transmitter

VI(b)BLOCK DIAGRAM FOR RECIEVER

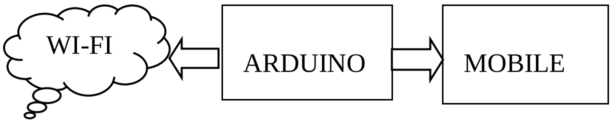


Fig2. Block diagram of Receiver

VII.ARDUINO UNO BOARD

Fig3:Arduino board

The Arduino Uno board is a microcontroller based on the AT mega 328 .it has 14 digital input /output pin in which 6 can be used as BWM output ,a 16MHZ ceramic resonator ,an ICSP header, a USB connection,6 analog input a power jack and a reset button This contains all the require support need for microcontroller . In order to get started ,they are simply connected to a computer with a USB cable or with aAC to DC adapted or battery. Arduino Uno board varies from all other board and they will not used the FTDI USB-to-serial driver chip in them .it is featured by the AT mega 16U2 programmed as a USB – to – serial converter

VIII. SYSTEM SETTINGS AND ALGORITHM USED

Here IR sensors are used, one should be placed right in front of the car and the other should be placed above the car. Used in the Arduino programming so that only if both the conditions are satisfied then only the Red Bulb/Indicator will grow indicating that the particular slot is occupied otherwise it will turn off and a Green bulb will glow showing that the slot is vacant. That is if any case if any person is changing in the parking slot then also it will be indicated as a vacant spot. To switch between Red Bulb and the Green Bulb a relay module is used which is triggered by the 5 Volt pin of the Arduino Board and to glow the bulb, an AC power supply is used, which will be connected to the relay module. The IR Sensors are used to eliminate and minimize any manual or human interference thus increasing the efficiency of the overall system.

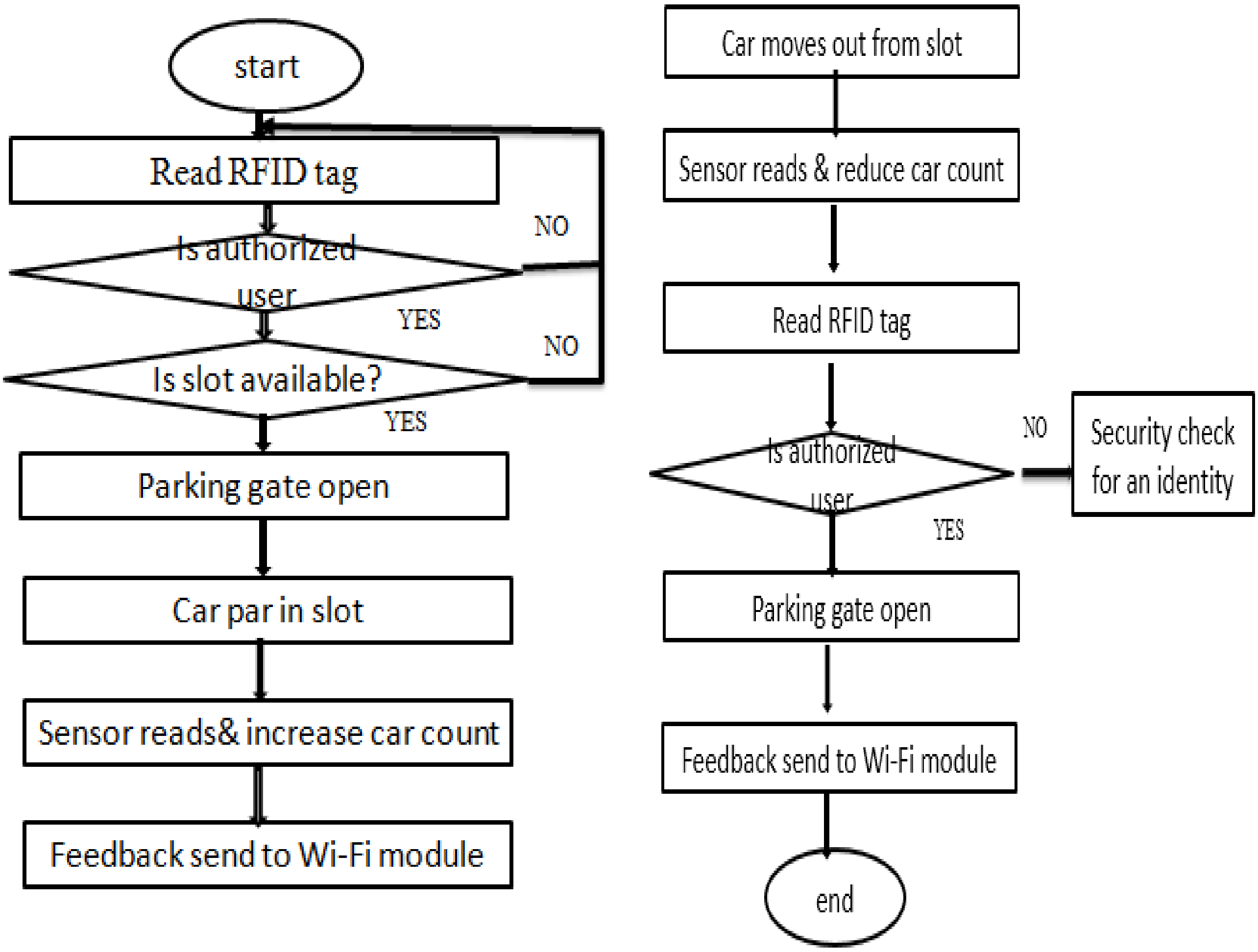
And finally, a Wi-Fi module is connected to the IR sensors. The Wi-Fi module should be first connected to the Internet that can be done through the AT commands of the ESP module. As soon as it gets connected to the Internet, it will receive the data from the Ultrasonic Sensor and send it to the IoT platform.

The ESP8266 is programmed using AT commands; when received, it replies with an acknowledgment. AT commands are a bit strange at first but with a little usage become easier to understand. These are run commands that run directly on the ESP module and are responsible for controlling the interaction between the ESP module and the Wi-Fi source.

There are many AT commands that can be used to program the ESP8266 Wi-Fi module. AT commands should be written in the Arduino's serial monitor to program the ESP8266. Some of them are listed below:

1) *"AT"* This will check if the module is connected properly and its functioning, the module will reply with an acknowledgment.
2) *"AT + CWLAP"* This will detect the Access points and their signal strengths available in the area.
3) *AT + CWJAP = "SSID"; "PASSWORD"* This connects the *ESP8266* to the specified *SSID* in the *AT* command mentioned in the previous code.
4) *"AT + RST"* This will reset the Wi-Fi module. Its good practice to reset it before or after it has been programmed. (OPTIONAL)
5) *"AT + GMR"* This will mention the firmware version installed on the ESP8266. (OPTIONAL)
6) *"AT + CIFSR"* This will display the ESP8266's obtained IP address. (OPTIONAL)
7) If the user wants to disconnect from any access point then use the following AT command: *AT + CWJAP = "";*

IX FLOWCHART



X.RESULTS

To obtain the perfect result, we set the IR sensor according to the parking lot dimensions in the Arduino code using Embedded C Programming. The problem faced during this research was that IR sensor was getting rust on its surface, thus leading the system to misbehave. Careful nano coating for sensors and the Arduino board is must for a long-term implementation of the project. Based on the data that the ESP is getting from the IR Sensor after connecting itself to a Wi-Fi through Arduino, it is successfully able to send the data to the open source platform.

XI. CONCLUSION

The status of the slot is shown with the help of the indicators and through IoT. The table 1 below shows the observation of the particular slot during the time of the day. In the table, various car models are shown, and the output is checked, thus confirming that the research was done up to the mark and showing the output correctly both in hardware and in software, irrespective of the car model.

XI. FUTURE SCOPE:

The future work focuses on the commercialization of a business prototype and to make a website more reliable using much better version of the ESP module, thus having a great business value as:

1.) A mobile application can be made instead of using the public IoT platform, to make it better for business purpose.
2.) The camera can also be connected, and number plate detection mechanism can also be implemented to make the area safer in terms of security.
3.) Online parking ticket system can also be implemented in the same setup

REFERENCES

[1] Guy Krasner and Eyal Katz,” Automatic parking iden-tification and vehicle guidance with road awareness”, IEEE

[2] Jae Kyu Suhr and Ho Gi Jung, “Automatic Parking Space Detection and Tracking for Underground and Indoor Environments”, IEEE Transactions on Industrial Electronics, 10.1109/TIE.2016.2558480

[3] P. Siva Nagendra Reddy, K. Tharun Kumar Reddy, P. Ajay Kumar Reddy, G. N. Kodanda Ramaiah and S. Nanda Kishor, “An IoT based home automation using android application”, 26 June 2017, International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), 2016,10.1109/SCOPES.2016.7955836

[4] Muhammed Onur Güngör, Yusuf Güngör and GökhanInce,”A secure wireless home automation system”, Signal Pro-cessing and Communications Applications Conference (SIU), 2017, 10.1109/SIU.2017.7960389

DESIGN AND IMPLEMENTATION OF REAL TIME TRANSFORMER HEALTH MONITORING SYSTEM USING GSM TECHNOLOGY

Mrs. V.SUDHA,
Assistant Professor
palanibalu.83@gmail.com
Electronics and Communication Engineering,
Krishnasamy College of Engineering and Technology, S.Kumarapuram, Cuddalore-607109

[1]v.Jaya Pragathi, [2]g.Sankavi, [3]l.Subhashini, PG Scholars

[1,2,3] M.E, (Communication System),
Krishnasamy College of Engineering and Technology, s.kumarapuram,cuddalore-607109
Email:, [1]ammupragathi1507@gmail.com, [2]sankavikrishnan@gmail.com,
[3]subhashiniece14@gamil.com

Abstract - This project is about design and implementation of a mobile embedded system to monitor and record key parameters of a distribution transformer like load currents, oil level and ambient temperature. The idea of on-line monitoring system integrates a Global Service Mobile (GSM) Modem, with a standalone Arduino and different sensors. It is installed at the distribution transformer site and the above parameters are recorded using the analog to digital converter (ADC) of the embedded system. The obtained parameters are processed and recorded in the system memory. If any abnormality or an emergency situation occurs the system sends SMS (short message service) messages to the mobile phones containing information about the abnormality according to some predefined instructions programmed in the microcontroller and also a new calling feature has been introduced in this system. This mobile system will help the transformers to operate smoothly and identify problems before any catastrophic failure.

Keyword - Transformer health Monitoring, Distribution Transformer, Power system fault.

I. INTRODUCTION

In power systems, distribution transformer is electrical equipment which distributes power to the low –voltage users directly, and its operation condition is an important component of the entire distribution network operation. Operation of distribution transformer under rated condition(as per specification in their nameplate) guarantees their long life .However their life is significantly reduced if they are subjected to overloading, resulting in unexpected failures and loss of supply to a large number of customers thus effecting system reliability. Overloading and ineffective cooling of transformers are the major causes of failure in distribution transformers. The monitoring devices or systems which are presently used for monitoring distribution transformers have some problems and deficiencies. Few of them are mentioned below.

1) Ordinary transformer measurement system generally detects a single transformer parameter, such as power, current, voltage. While some ways could detect multi- parameter, the time of acquisition and operation parameters is too long, and testing speed is not fast enough.

2) Detection system itself is not reliable. The main performance is the device itself instability, poor anti-jamming capability, low measurement accuracy of the data, or even state monitoring system should is no effect.

3) Timely detection data will not be sent to monitoring centres in time, which cannot judge distribution transformers three-phase equilibrium
4) A monitoring system can only monitor the operation state or guard.
5) Against steal the power, and is not able to monitor all useful data of distribution transformers to reduce costs.

Many monitoring systems use power carrier communication to send data, but the power carrier communication has some disadvantages: serious frequency interference, with the increase in distance the signal attenuation serious, load changes brought about large electrical noise. So if use power carrier communication to send data, the real-time data transmission, reliability cannot be guaranteed.

According to the above requirements, we need a distribution transformer real-time monitoring system to detect all operating parameters operation, and send to the monitoring centre in time. It leads to online monitoring of key operational parameters of distribution transformers which can provide useful information about the health of transformers which will help the utilities to optimally use their transformers and keep the asset in operation for a longer period. This will help to identify problems before any serious failure which leads to a significant cost savings and greater reliability. Widespread use of mobile networks and GSM devices such GSM modems and their decreasing costs have made them attractive options not only for voice media but for other wide are network applications.

II. TRANSFORMER FAULT ANALYSIS

A power transformer consists of a set of windings around a magnetic core. The windings are insulated from each other and the core. Operational stresses can cause failure of the transformer winding, insulation, and core. The power transformer windings and magnetic core are subject to a number of different forces during operation:

1. Vibration caused by flux in the core changing direction
2. Localized heating caused by eddy currents in parts of the winding, induced by magnetic flux
3. Impact forces caused by fault currents.
4. Thermal heating caused by overloading.

These operating limits only considered the thermal effects of transformer overload. Later, the capability limit was changed to include the mechanical effect of higher fault currents through the transformer. Power transformer faults produce physical forces that cause insulation wear. These effects are cumulative and should be considered over the life of the transformer. The following discussion highlights on different capability limits of transformer.

2.1 Over Load

Over Load Over current is the current flowing through the transformer resulting from faults on the power system. Fault currents that do not include ground are generally in excess of four times full-load current; fault currents that include ground can be below the full-load current depending on the system grounding method. Over current conditions are typically short in duration (less than two seconds) because protection relays usually operate to isolate the faults from the power system. Overload, by contrast, is current drawn by load, a load current in excess of the transformer nameplate rating. In summary, loading large power transformers beyond nameplate ratings can result in reduced dielectric integrity, thermal runaway condition (extreme case) of the contacts of the tap changer, and reduced mechanical strength in insulation of conductors and the transformer structure. Three factors, namely water, oxygen, and heat, determine the insulation life of a transformer. Filters and other oil preservation systems control the water and oxygen content in the insulation, but heat is essentially a function of the ambient temperature and the load current. Current increases the hottest-spot temperature (and the oil temperature), and thereby decreases the insulation life span.

2.2 Temperature

Excessive load current alone may not result in damage to the transformer if the absolute temperature of the windings and transformer oil remains within specified limits. Transformer ratings are based on a 24-hour average ambient temperature of 30°C (86°F). Due to over voltage and over current, temperature of oil increases which causes failure of insulation of transformer winding.

2.3 Over/Under Voltage

The flux in the transformer core is directly proportional to the applied voltage and inversely proportional to the frequency. Over voltage can occur when the per-unit ratio of voltage to frequency (Volts/Hz) exceeds 1.05 p .u at full load and 1.10 p.u. at no load. An increase in transformer terminal voltage or a decrease in frequency will result in an increase in the flux. Over excitation results in excess flux, which causes transformer heating and increases exciting current, noise, and vibration.

2.4 Oil Level Fault

Oil mainly used in transformer for two purposes one is for cooling of transformer and another use is for insulation purpose. When temperature of transformer goes high, oil level in transformer tank decreases due to heating effect. For normal operation of transformer oil level should maintain at required level. If oil level decreases beyond required level, it affect cooling and insulation of the transformer.

III. THE ARDUINO MEGA 2560

It is a microcontroller board based on the AT-Mega 2560 (datasheet). It has 54 digital input/output pins (of which 14 can be used as PWM outputs), 16 analog inputs, 4 UARTs (hardware serial ports), a 16 MHz crystal oscillator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started. The Mega is compatible with most shields designed for the Arduino Duemilanove or Diecimila.

Schematic & Reference Design EAGLE files:

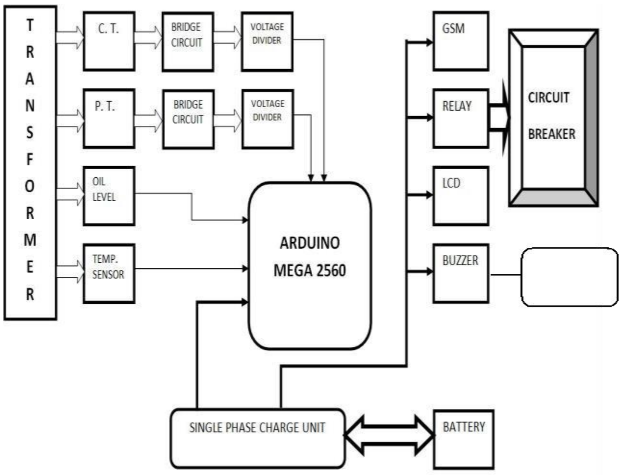
Arduino-mega2560-reference-design.zip **Schematic:** arduino-mega2560-schematic

Summary

Microcontroller ATmega2560 Operating Voltage 5V
Input Voltage (recommended) 7-12V Input Voltage (limits) 6-20V
Digital I/O Pins 54 (of which 14 provide PWM output)
Analog Input Pins 16
DC Current per I/O Pin 40 ma DC Current for 3.3V Pin 50 ma
Flash Memory 256 KB of which 8 KB used by boot-
loader

SRAM 8 KB
EEPROM 4 KB
Clock Speed 16 MHz
Power The Arduino Mega can be powered via the USB connection or with an external power supply. The power source is selected automatically.

IV. DESIGN OF ARDUINO BASED TRANSFORMER HEALTH CONDITION MONITORING KIT



It consist of current transformer, power transformer, thermister, oil sensor, Arduino, LCD display, GSM modem and relay. Normally in transformer, failure occurs due to voltage and current fluctuation, overheating, change in oil level etc. In this project, to sense these fault we have used current and power transformer, temperature sensor, oil sensor respectively. All these sensors are connected Arduino. GSM model and LCD respectively. When fault occurs due to above any reason then change in ratings will be shown on LCD and quick SMS will go to control room via GSM modem. A brief discussion about components used is as given below Sensors play a vital role in effective implementation of the project. As we are interested in monitoring over current, over temperature and oil level following sensors are selected and suitable designed with respect to prevailing conditions of power system and rating of transformer to be protected.

4.1 Current and Voltage Transformer

Current or potential transformers are necessary for isolating the protection & control. The behaviour of current and voltage transformer during and after the occurrence of fault is critical in electrical protection since error in signal from transformer can cause mal operation of the relays.

4.2 Oil Level Sensor

Oil level sensor is float connected angular potentiometer. Float is immersed in oil and its mechanical output is given to angular potentiometer. When there is any mechanical movement of float, there is voltage generation corresponding to mechanical movement of float. That voltage is used for oil level monitoring.

4.3 Temperature Sensors LM35

4.3.1 Feature

- ✓Calibrated directly in□^{0}Celsius (Centigrade)
- ✓ Linear a 10.0 mV/§C scale factor ✓ 0.5 ^{0}C accuracy guarantee able (at a25^{0}C)
- ✓ Rated for full b55 ^{0}C to a150 ^{0}C range
- ✓ Suitable for remote applications□
- ✓ Low cost due to water-level trimming□
- ✓ Operates from 4 to 30 volts□
- ✓ Less than 60 mA current drain□
- ✓ Low self-heating, 0.08 ^{0}C in still air□
- ✓ Low impedance output, 0.1 X□

4.3.2 Applications

The LM35 can be applied easily in the same way as other Integrated- circuit temperature sensors. It can be glued or cemented -to a surface and its temperature
will be within about 0.01^{0}C of the surface temperature.
This presumes that the ambient air temperature is almost the same as the surface temperature; if the air temperature were much higher or lower than the surface temperature the actual temperature of the LM35 die would be at an intermediate temperature between the surface temperature and the air temperature. This is especially true for the TO-92 plastic package, where the copper leads are the principal thermal path to carry heat into the device, so its temperature eight be closer to the air temperature than to the surface temperature.

To minimize this problem, be sure that the wiring to the LM35, as it leaves the device, is held at the same temperature as the surface of interest. The easiest way to do this is to cover up these wires with a bead of epoxy which will insure that the leads and wires are all at the same temperature as the surface, and that the LM35 die's temperature will not be affected by the air temperature.

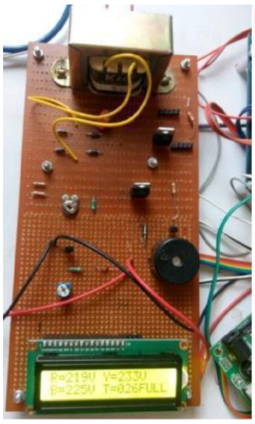
5. CASE STUDY

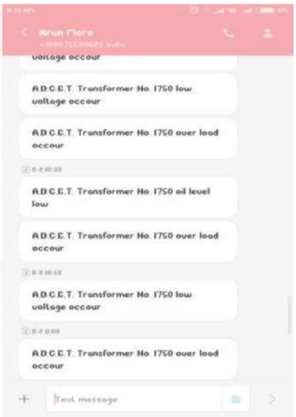
- ✓ This system is totally independent i.e. having separate power supply to operate this total circuitry which is nothing but battery supplied.□
- ✓ This system can sustain over up-to 66 kV range.
  - ➢ Over these voltages there is some restriction about CT and PT ratio. As the ratio increases, change in output i.e. secondary output has large change which cannot directly proportional to input quantity.
  - ➢ Limit range of voltage level such as minimum and maximum can set which is in our hand so that we can decide the range of voltages.
  - ➢ Similarly we can set the maximum limit of current so that crossed limit is abnormal current range.
  - ➢ Even having single line taking large current than other lines and set limit will also takes as faulty condition.
  - ➢ We also have the oil level detector having full and low indication. It indicates that whenever the oil inside of transformer goes low or particular set limit it will give indication.
  - ➢ We attached temperature detector too for checking the condition of transformer overall body temperature. Even that sensor can act like temperature sensor of oil inside of transformer where it is inserted in oil of transformer.

- This system can be also used in **Transmission Line, and Three Phase Induction Motor.** Only exception is oil level sensor and temperature sensor, we can take it as neutral in those above cases.

- If any abnormal condition occur mentioned above, it will give indication through buzzer and will cut the system supply or load through line and inform us through GSM message which fault occurs on system□

6. RESULT





voltage occour

A.D.C.E.T. Transformer No. 1750 low voltage occour

A.D.C.E.T. Transformer No. 1750 over load occour

A.D.C.E.T. Transformer No. 1750 oil level low

A.D.C.E.T. Transformer No. 1750 over load occour

A.D.C.E.T. Transformer No. 1750 low voltage occour

A.D.C.E.T. Transformer No. 1750 over load occour

Fault No.1- Voltage level

When device detects low voltage or high voltage (set values), it will send the message to set number that "Transformer no.--- Low/High Voltage Occur", also it will trigger circuit breaker for cut off supply.

Fault No. 2- Over Load

When device detects current flowing through system high then it assumed that system is overloaded. After detect overloading device send message "Transformer No. --- Overload Occur", and will break system through line by opening circuit breaker.

Fault No.3- Oil Level

In this system in transformer oil level is low or high it sense the by using float sensor it gives the massage through GSM by mobile.

Fault No.4-

Temperature Ambient temperature of Transformer is high or it will be increase it sense through the sensor LM-35 and gives msg. through GSM by mobile.

CONCLUSION

Transformers are among the most generic and expensive piece of equipment of the transmission and distribution system. Regular monitoring health condition of transformer not only is economical also adds to increased reliability. In the past, maintenance of transformers was done based on a pre-determined schedule. With the advancement of communication technology now it is possible to receive fault information of transformer through GSM technology remotely to the operator and authorities so one can able to take possible solution before converting fault in to fatal situation. Depending upon fault analysis a prototype model of microcontroller based transformer health monitoring kit is developed in laboratory. Using digital controller analysis results are regularly updated. During abnormal conditions exceeding specified limits information is immediately communicated through GSM technology to the operator and also to concerned authority for possible remedial action. This type of remote observation of health condition of transformer not only increases the life of transformer but also increases mean down time of transformer there by increased reliability and decreased cost of power system operations.

REFERENCES

[1] Vadirajacharya. K, Ashish Kharche, Harish Kulakarni, Vivek
Landage "Transformer Health Condition Monitoring Through GSM Technology", International Journal of Scientific &
Engineering Research Volume 3, Issue 12, December-2012

[2] ANURUDH KUMAR1, ASHISH RAJ2, ABHISHEK KUMAR3, SIKANDAR PRASAD4 & BALWANT
KUMAR.5 "METHOD FOR MONITORING OF DISTRIBUTION TRANSFORMER",1,2,3,4 &5 Dr. M.G.R,
Educational and Research Institute, University, Chennai-600095.

[3] U.V.Patil1, Kathe Mohan2, Harkal Saurabh3, Warhade Nilesh4 "Transformer Health Condition Monitoring Using GSM Technology", Vol-2 Issue-2 2016 IJARIIE,

[4] A. Z. Loko1, A. I. Bugaje2, A. A. Bature3 "AUTOMATIC
METHOD OF PROTECTING TRANSFORMER USING PIC MICROCONTROLLER AS AN ALTERNATIVE TO THE FUSE PROTECTION TECHNIQUE", International Journal of Technical Research and Applications e-ISSN: 2320-8163, Volume 3, Issue 2 (Mar-Apr 2015), PP. 23-27.

[5] Karpe S R1, Sandeep Shelar2, Shraddha Garkad3, Shruti Lakade4 "Fault Detection and Protection of Transformer by Using Microcontroller", International Journal of Modern Trends in Engineering and Research.

Advanced power distribution system with economic management by using RF technology

Kavisree.T
Assistant Professor,
Department of Electronics and communication Engineering,
AKT Memorial college of Engineering& Technology,
Kallakurichi– 606202.
Kavisree273@gmail.com

[1]Mmuthulakshmi.K, [2]Priya.P, [3]Sathiya.S
[1,2,3] UG students,
Department of Electronics and communication Engineering,
AKT Memorial college of Engineering& Technology,
Kallakurichi– 606202.

***Abstract*—In recent years, power management and power economic management is one of the hot topic and the power shutdown is a major issue for domestic power consumers, to avoid this problem an EB central computer transmit power in an essential mode i.e transmitting uninterrupted power without power cut and mainly there is no use of UPS system. In this essential mode it delivers a minimum current only, if the user reaches beyond the essential load automatically its shutdown the outgoing distribution line by using electrical relays in energy meter, in business we can save power and to distribute uninterrupted power in our country by using this system.**

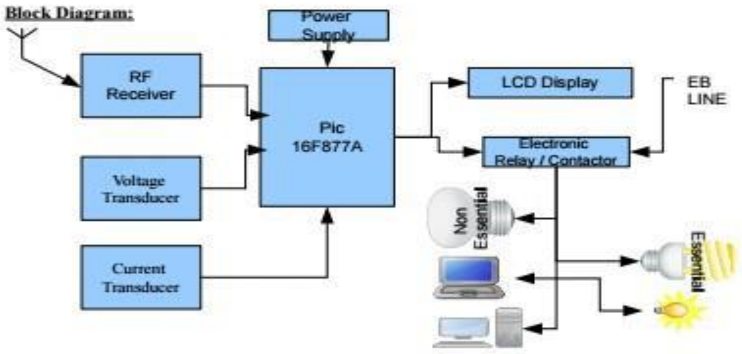
Keywords- ZigBee, economic load dispatching, loading identification.

I. INTRODUCTION

Global warming phenomenon is getting worse day by day. Weather in every place of the world is becoming very abnormal. Ice zone of north and south poles is melting in very fast speed. El Nino causes significant meteorological disaster. People begin to have subconscious of energy crisis and protect the world commonly depended by all of us. People also try to green the surrounding environment. The issues of implementing energy-saving and emission-reducing is seemed better to be brooked no delay.

In modern life, every electric product need to use the plug to plug into the outlet to acquire electricity in addition to use battery. Therefore, plug is equal to power usage. If we can add an energy-saving device to the electric plug being used and assign a unique name to be identified, then we can learn its name and details of power usage through this energy-saving plug. Interfacing this energy-saving plug with populous wireless equipment nowadays, the host computer in the house can easily to know power usage in the area and power consumption of electric products and to control them. By way of simple setting, applications of power saving and security management can be implemented. Power saving can reduce money payment. In security, it provides an additional protection for the electric product. This integration also reaches the goal of energy-saving and emission-reducing [1][2].

Voltage, current and power factor are detected from the load side and theses data are transmitted to the host computer side. Electricity consumption of the load side is analyzed by using computer program. By arranging area energy-saving plug, individual setting and status examining of every plug can be executed. This also includes multiple settings and managing manners of different date and period. We can easily use this system to estimate the electricity charges of current month. Beside! Effectively control the electricity consumption of a family, the usage situation of electricity can be obtained at any time to avoid electrical fire and other accidents to happen. Of course, the stability of the system should be strictly checked to correct defects and to increase safety. Furthermore, this system is intended to the vanguard weapon of implementing load identification and energy management![3].



As shown in Figure 1, that sensing components are used to process measurement of voltage and current is clearly indicated in the block diagram of the monitoring system. Microprocessor and wireless device are used to receive and transmit data. By using computer, analyzing and monitoring are executed.

II. CONTROL METHODS OF THE SYSTEM

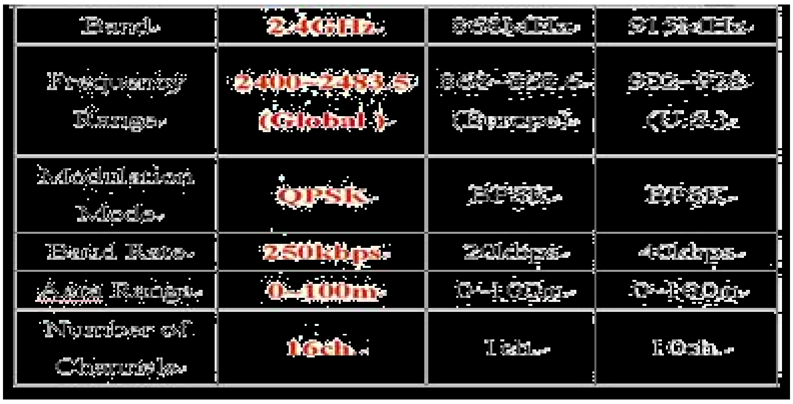
Internet is accompanied with the progress of network media, Micro electro-mechanics, and nano integrated circuits technologies to make wireless communication technique to become mature and to make a breakthrough. Advanced countries in the world all actively develop ubiquitous network structure. It is hopefully by combining and applying different kinds of wireless network communication techniques to interweave one closely related information and communication network to bring more security and convenience for human daily life..

.

A. ZigBee Wireless Transmitting System

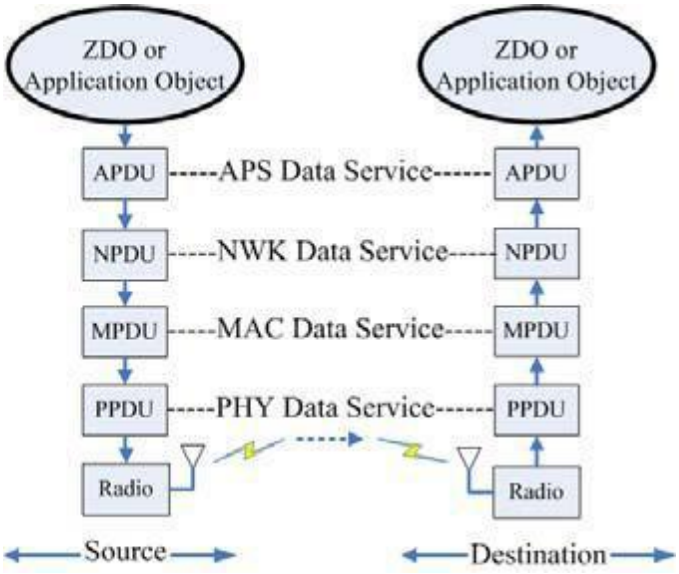
ZigBee is based on 802.15.4 which is established by IEEE. It is a new standard of short-distance wireless communication transmission. It emphasizes on characteristics of low cost, small power consumption, two-way transmission function. Its transmission distance is several ten meters. The data rate in the band of 2.4GHz is 250Kbps. Its characteristics in 868/915MHz are illustrated in Table 1. The technology of ZigBee is a wireless network transmission in point-to-point cascaded connection. It is applied to applications of low speed, low power and short distance. By using a remote controller or a communicating equipment, it is possible to control air conditioners, lighting equipments, fire protection system and other home appliances in the whole area. [4][5]

TABLE I.
DIFFERENCES AMONG BANDS OF 2.4GHZ, 868 MHZ AND 915MHZ



Band	2.4GHz	868MHz	915MHz
Frequency Range	2400~2483.5 (Global)	868~868.6 (Europe)	902~928 (U.S.)
Modulation Mode	QPSK	BPSK	BPSK
Baud Rate	250kbps	20kbps	40kbps
Area Range	0~100m	0~100m	0~100m
Number of Channels	16ch	1ch	10ch

The basic reference model of Open Systems Interconnection (OSI) is six layers. Under the simplification of the IEEE802.15.4 and ZigBee alliance, the framework of ZigBee is divided into five layers as follows: Physical Layer (PHY), Medium Access Control Layer (MAC), Logical Link Control (LLC), Network Layer (NWK), Transport Lay (TAN) and Application Layer (APL) as shown in Figure 2. Packets are transmitted in the way of stacking. The information of each layer is stacked into the packet in order to transmit.



Packets receive hardware information or dpnnboet! from APS the layer. They are stacked with roles of network equipments in the NWK layer and address information of equipments in MAC layer. Then, they are stacked with settings in the PHY layer to send out the packet. After packets are received, they are confirmed by the PHY layer and they are ascertained by the addresses of the MAC layer and role definition in the NWK layer to affirm if the packets want to give commands to this equipment or to other equipment. If not, then skip directly. If packets are belonged to this equipment, then they are resolved by the APS layer to directly execute commands and transmit information with the hardware equipment. Transformations of data between equipment are indicated in Figure 3.

memory resource required by the system is at least 32 kbytes (for the 8-bit controller). Time needed for very new secondary node is more than 30ms. The ZigBee system is sufficient to provide the usage of 256 electric appliances. It is able for fast connection, information interchange, separation, and then back to waiting and sleeping status for the purpose of acquiring longer life time for batteries.

B. Features of the ZigBee Technology

Power Saving: The transmission speed is low and quantity of transmitted data is also low. Therefore, the access time of signal is short. In no operating mode, ZigBee is in waiting mode. The switching time between operation and waiting mode is described as follows: general time needed from waiting to starting is only 15 ms. Time for finding an equipment is 30 ms. Hence, ZigBee is known to be power saving. Using battery in ZigBee can be with life time of 6 months to two years or so.

High reliability: the function of talk-when-ready collision avoidance is adopted by the MAC layer of ZigBee. This function is to send data immediately when data are requested to be transmitted. Arrival of every transmitted data packets is confirmed by the receiving side. If the confirmed message is not got, then it means that collision is occurred. It is needed to retransmit

VI DISCUSSIONS AND CONCLUSIONS

From This Study, Hereafter There is no Power Shutdown Problem. There Will be an Uninterrupted. Power Supply to domestic Purpose. This Study provides PIC Microcontroller Which Inbuilt ADC&DAC and also it is very faster when compared to other Micro.

REFERENCES

[1] Ching-Lung Lin, Yuan-Chuen Hwang, Ching-Feng Lin, "Development of A Hierarchical Saving Power System for Campus", in *Proceedings of the* 13th International Conference on Computer Supported Cooperative Work in *Design*, Chile, pp.746-750, April 22-24, 2009

[2] Hsueh-Hsien Chang, Ching-Lung Lin, and Lin-Song Weng, "Application of Artificial Intelligence and Non-Intrusive Energy-managing System to Economic Dispatch Strategy for Cogeneration System and Utility", in *Proceedings of the 13thInternational Conference on Computer Supported Cooperative Work in Design*, Chile, pp. 740-745, April 22-24, 2009

[3] Su Kai, Li Qing, Liu Jizhen, Niu Yuguang, Shi Ruifeng Bai Yang, "New Combination Strategy of Genetic and Tabu Algorithm an Economic Load Dispatching Case Study", in *Proceedings of the2011 Chinese Control and Decision Conference (CCDC)*, China, pp.1991-1995, 2010.

[4] Daniel Alexandru Vi an, Ioan Li, Mariana Jurian and Ion Bogdan Cioc, "Wireless Measurement System Based on ZigBee Transmission Technology", in *The 33rd International SpringSeminar on Electronics Technology*, pp. 464-467, 2010

[5] Hsueh-Hsien Chang, and Ching-Lung Lin, "A New Method for Load Identification of Nonintrusive Energy Management System in Smart Home", in *Proceeding of IEEE InternationalConference on e-Business Engineering, China*, 2010

[6] Wan-Ki Park; Chang-Sic Choi; Jinsoo Han; Han, I., "Design and Implementation of ZigBee based URC Applicable to Legacy Home Appliances", in *IEEE International Symposium onConsumer Electronics*, pp. 1-6, 2007

Frequency and Beam Reconfigurable Monopole Antenna using VARACTOR Diode

[1]rajakumaran.n, [2]sivasitrarasu.S, [3]muthukumaran.J. K
[1,2,3] UG students,
Department of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

B. Mary Amala Jenni,
Assistant Professor,
Department of Electronics and Communication Engineering
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

M. Vaidehi,
Professor,
Department of Electronics and Communication Engineering
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Abstract**—** A novel frequency and pattern reconfigurable monopole antenna is designed in this paper. The reconcilability is achieved by integrating an active frequency selective surface (AFSS) with feed antenna. A monopole Antenna is designed to illuminate AFSS, The smart FSS comprises a printed slot array loaded by varactors The Varactor diodes are placed in the AFSS such that the reconfigurable is achieved by switching on &off. The varactor diode the proposed design work at 2 different frequencies and power consumed is very less. Antenna design is other switches like PIN diode. A monopole antenna is designed to illuminate the AFSS. The resulting structure can operate in a frequency tuning range of 30%. By reconfiguring the different sections of active FSS cylinder into a transparent or reflector mode, the omnidirectional pattern of the source antenna can be converted to a directive beam. Experimental results demonstrate the capability of providing useful gain levels and good impedance matching from 1.7 to 2.3 GHz. The antenna offers a low-cost, low-power solution for wireless systems that require frequency and beam reconfigurable antennas. The proposed design consumes about 1000 times less dc power than the equivalent narrowband beam-switching antenna design using p-i-n diode-loaded AFSS.

Index Terms**— Beam steering, frequency and beam reconfigurable, frequency selective surface (FSS), frequency tunable, reconfigurable antennas.**

I. INTRODUCTION

Future wireless networks are going to evolve to provide significant improvements, such as higher data rates, reduced end-to-end latency, and lower power Consumption. Most wireless systems employ multiple antennas, which can lead to increased hardware complexity, large size, high power consumption, and high cost. Reconfigurable antennas with the capacity to electronically alter their operating modes, have been extensively studied during the past few decades. Such reconfigurable antennas are important for achieving optimum performance of wireless systems under various environmental conditions. Compared with frequency-switched antennas, which operate at some predefined separate frequency bands frequency- tunable antennas can achieve dynamic control of relatively narrow instantaneous bandwidths, and thus allowing operation over a larger bandwidth. Various continuous frequency tuning techniques employing varactors can be found in the literature dual-band reconfigurable slot antenna is presented in, where two varactors are placed in appropriate locations of the slot to achieve dual-frequency operation. Hum and Xiong Propose a differentially fed, frequency agile patch antenna incorporating three pairs of varactors. The tuning range for −10-dB reflection coefficient is approximately from 1.8 to 3.15 GHz. Reference presents acoplanar waveguide wideband monopole antenna integrated with a frequency tunable bandpass. The resulting antenna is demonstrated to have a tuning range from 2.88 to 4.62 GHz and a 50% gain reduction at the higher frequencies. Despite continuous frequency tuning, the beams of the reported antennas in all fixed.

Pattern reconfigurable antennas, on the other hand, can be exploited as a cost-effective substitute for conventional phased arrays that consist of expensive RF components, such as phase shifters and amplifiers. By subtly steering the antenna main beam toward the intended users, a pattern reconfigurable antenna can be used to suppress multipath fading and increase channel capacity. Much work has been done to design low-cost, pattern reconfigurable antennas incorporating RF switches However, there are few solutions available for combining both frequency and pattern configurability into a single antenna structure. A frequency-agile, switched- beam antenna array described in is capable of switching four beams using switched line phase shifters. But the antenna can only operate at two fixed frequencies (4.7 and 7.5 GHz). The combination of frequency and pattern configurability into the same antenna leads to a simplify and highly integrated solution for size-constrained multifunction platforms where diversity schemes are employed to improve the system performance, for example, in multiple input multiple-output communication systems.

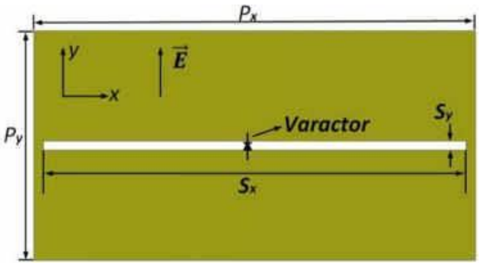


Fig. 1. Schematic of the ideal all-metal unit cell.

II. ACTIVE FSS DESIGN

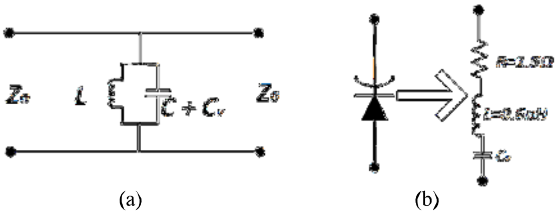


Fig. 2. EC model of (a) tunable unit cell and (b) varactor diode.

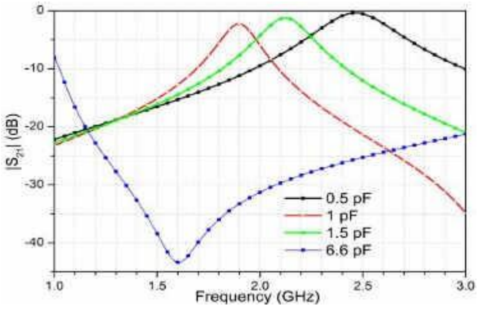


Fig. 3. Simulated transmission coefficient of the ideal unit cell.

To fully understand the tuning mechanism of the FSS, an equivalent circuit (EC) model is used as a simpler and faster method than full-wave simulation in CST. Fig. 2(a) shows the EC model derived from transmission line analogy. Essentially, the EC model is simply a parallel *LC* circuit. The inductance is associated with the electric current fl wing in the patch and the capacitance consists of an intrinsic capacitance *C* between the gap of the slot and the variable capacitance C_{V} from the varactor diode. According to the bandpass filter theory, the resonance frequency of the FSS can be expressed as follows:

A. *Ideal FSS Unit Cell Analysis and Modeling*

As a preliminary examination of the tunability of the slot FSS, an ideal all-metal unit cell is simulated using the Floquet mode of the frequency domain solver in CST. The metal-only FSS unit cell consists of a half-wavelength slot in the center of a copper plate, as shown in Fig. 1. A varactor is connected

between the gap and the physical bias circuit is excluded for simplicity. The dimensions of the unit cell in Fig. 1 are $P_x = 48$ mm, $P_y = 25$ mm, $S_x = 46$ mm, and $S_y = 0.2$ mm. The slot FSS is a relatively simple structure, which makes it

a good option for AFSS design as it comparatively lowers the complexity of the biasing circuit.

$$f = 1/[2\pi \quad L(C + C\text{v})]. \qquad (1)$$

It is clear that from (1), increasing the capacitance of the varactor shifts the resonance frequency downward. The tuning range is limited by the capacitance ratio of the varactor. Normally, higher ratios yield wider frequency tuning ranges. Here, we used an Infineon BB857 silicon varactor whose capacitance tunable range is from 0.52 to 6.6 pF. To simplify the simulation, the varactor is modeled as a series *RLC* circuit with a series inductance of 0.6 nH and resistance of 1.5 , as shown in Fig. 2(b). Fig. 3 shows the simulated transmission coefficients of the ideal slot FSS without bias network for different capacitance values. It can be noted that by varying the capacitance from 0.5 to 1.5 pF, the slot resonance frequency can be tuned from 2.5 to 1.9 GHz with an acceptable transmission level. More importantly, the curve for 6.6 pF shows that between 1.2 and 3 GHz, the S_{21} level is below −20 dB, which means almost no EM wave can be transmitted through the FSS. This is an extremely good feature for reconfiguring the FSS as a reflector, which is explored for the eventual structure.

B. *Bias Network Design*

The bias network is the most critical part of the active FSS design. Maintaining a simple network is beneficial for minimizing the unwanted effect caused by the bias lines. In our

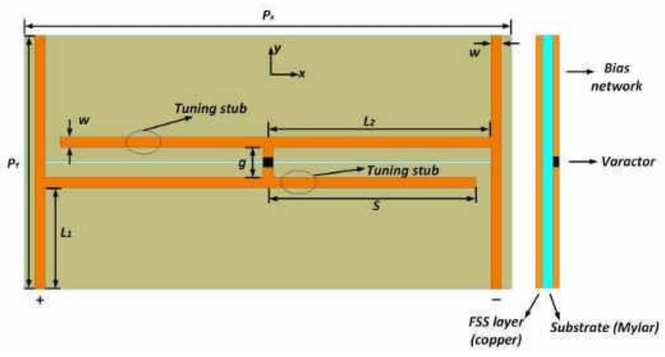
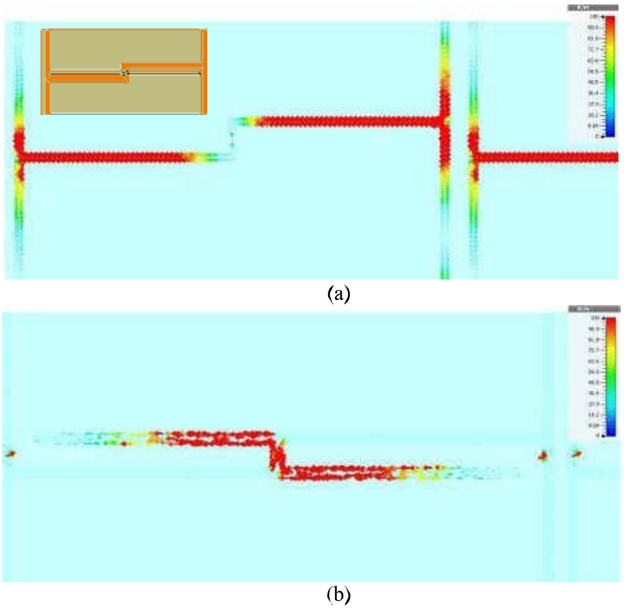


Fig. 4. Schematic of the resulting bias network.



(a)

(b)

TABLE I

BIAS NETWORK DIMENSIONS [mm]

L_1	L_2	w	g	S	P_x	P_y
10.5	22.5	1	2	20.5	48	25

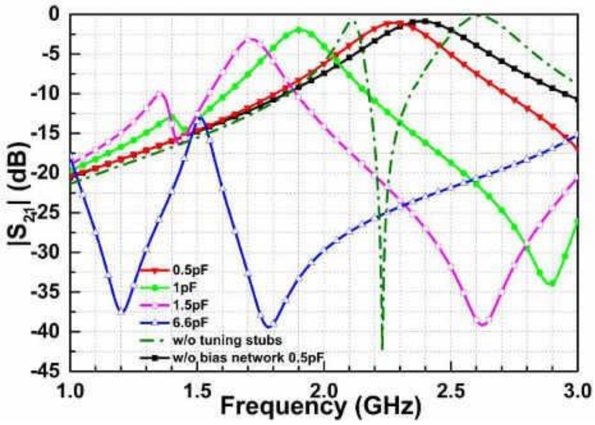


Fig. 5. Simulated transmission coefficients of the unit cell with bias network.

III. FREQUENCY TUNABLE ANTENNA DESIGN

After the investigation of the planar active FSS, the next step is to integrate it with a feed antenna. The planar FSS is rolled into a cylinder to mimic a corner reflector antenna.

TABLE II

METALLIC REFLECTOR ANTENNA DIMENSIONS [mm]

D	h_1	h_2	G	t	R_g	R_c	H
37	50	40	2	0.5	74	76	200

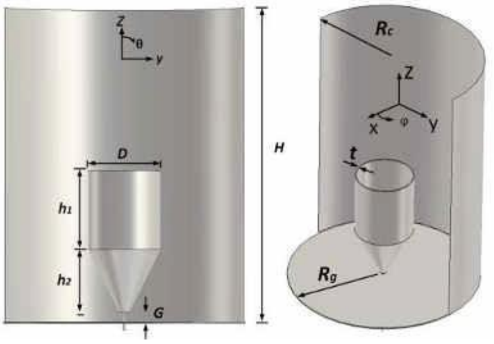


Fig. 67. Schematic of the metallic reflector antenna.

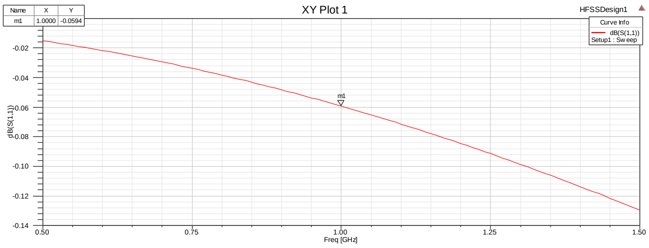


Fig.7. Simulated reflection coefficient and gain of the reference antenna.

A. *Metallic Reflector Antenna*

It is necessary to investigate the reflector antenna to give some design guidance about the influence of AFSS size, feeder dimensions, and so on. A conical monopole antenna is used as the radiator, as shown in Fig. 7. The dimensions of the reflect antenna are given in Table II.

The metallic reflector antenna is used as a reference and optimized to have stable performance in terms of impedance matching and gain. Fig. 8 shows the simulated reflection coefficient and gain of the antenna. The operating frequency covers 1.5–2.7 GHz. It can be noted that the gain rises gradually owing to the increased aperture size. The computed radiation patterns are shown in Fig. 9.

B. *AFSS Antenna Design*

The parameters of the reference antenna, R_C and H (Table II), can be used as the initial values for the active FSS cylinder design. Before rolling the planar FSS into a cylinder, the number of unit cells along the circumference and axis is deduced from the following equations:

$$N_X = 2\pi \times R_C / P_X \qquad (2)$$

$$N_y = H / P_y\,. \qquad (3)$$

The final structure consisted of 10 columns and 8 rows, as shown in Fig. 10. Note that a half cylindrical AFSS and diodes have been made transparent in Fig. 10 for clarity. The dimensions of the resulting antenna are the same as those of the metallic reflector antenna except that the reflector is replaced by the cylindrical AFSS

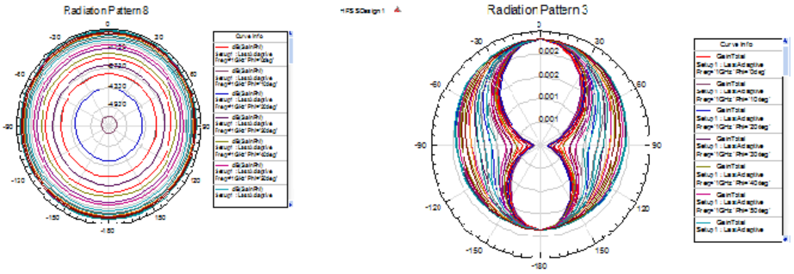


Fig. 8. Simulated radiation patterns of the reference antenna.

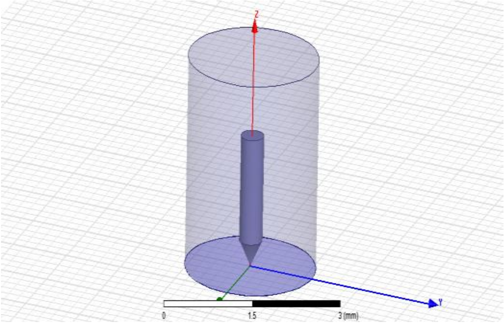
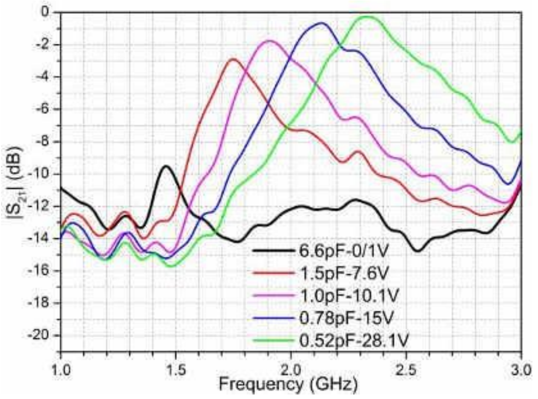
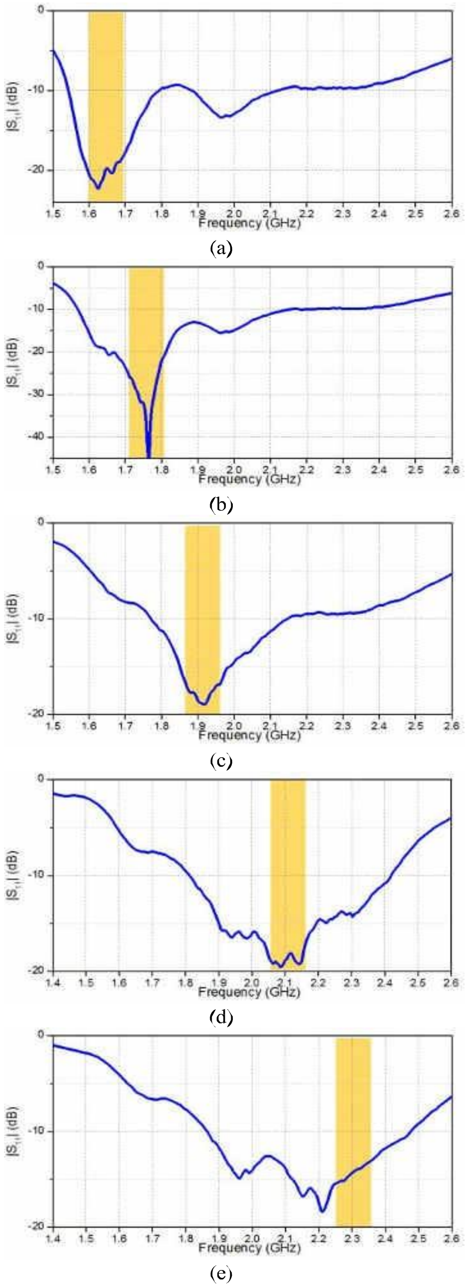


Fig. 9. Schematic of the final antenna structure.



.

Fig.10. Measured transmission coefficients of the tunable FSS.



(a)

(b)

(c)

(d)

(e)

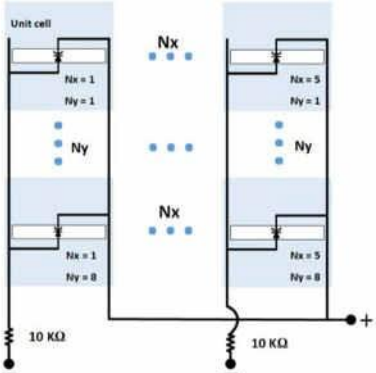


Fig. 11. Schematic of the bias network of half AFSS.

Fig. 12. Measured antenna reflection coefficients at (a) 7, (b) 8, (c)10.1,(d) 15, and (e) 28.1 V.

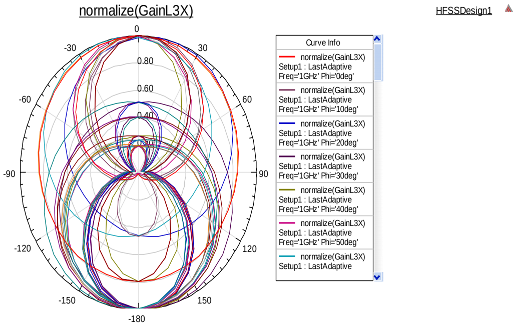


Fig. 13. Measured switched beams at 1.9 GHz in the H-plane.

IV CONCLUSION

The frequency tuning and beam switching characteristics of a novel antenna have been presented. A slot FSS array incorporating varactor diodes is employed to produce the passband tunability. When integrated with a feed antenna, the impedance matching and peak gain of the antenna can be tuned by varying the applied dc voltages. The achieved 30% continuous tuning range results in a wider operation bandwidth than conventional FSS beam-switching antennas. Measured results show the realized gain varies from 7.4 to 10 dBi over the entire frequency tuning range. The antenna tuning bandwidth is limited by the varactor capacitance ratio, which determines the tuning range of the slot FSS. To the best of our knowledge, this is the first time a dc power consumption comparison has been undertaken for the beam-switching antenna applications using AFSS. The proposed antenna has a low cost and requires very low power to operate in its various states, and thus, it is a promising candidate for future wireless communication applications in which low cost and low power are required.

REFERENCES

[1] J. Costantine, Y. Tawk, S. E. Barbin, and C. G. Christodoulou, "Recon- fi Antennas: Design and Applications," *Proc. IEEE*, vol. 103, no. 3, pp. 424–437, Mar. 2015.

[2] C. G. Christodoulou, Y. Tawk, S. A. Lane, and S. R. Erwin, "Recon- fi antennas for wireless and space applications," *Proc. IEEE*, vol. 100, no. 7, pp. 2250–2261, Jul. 2012.

[3] W. A. Imbriale, S. Gao, and L. Boccia, *Space Antenna Handbook.* Hoboken, NJ, USA: Wiley, 2012.

Combining Memory Allocation and Processor Voltage Scaling for Energy-Efficient IoT Task Scheduling

Ms.S.K.Suriya, Assistant Professor,
Department of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Mrs.D.Umamaheshwari, Associate Professor,
Department of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Mrs.C.Suganya, Assistant Professor,
Department of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Abstract* — As IoT (Internet-of-things) technologies grow rapidly for emerging applications such as smart living and health care, reducing power consumption in battery -based IoT devices becomes an important issue. An IoT device is a kind of real-time systems, of which power-savings have been widely studied in terms of processor's dynamic voltage/frequency scaling. However, recent research has shown that memory subsystems are G getting reached to a significant portion of power consumption in such systems. In this paper, we show that power consumption of real-time systems can be further reduced by combining voltage/frequency scaling with task allocation in hybrid memory. If a task set is schedulable in a low voltage mode of a processor, we can expect that the task set will still be schedulable even with slow memory. By considering this, we adopt non-volatile memory technologies that consume less power than DRAM but provide relatively slow access latency. Our aim is to allocate tasks in non-volatile memory if it does not violate the deadline constraint of real-time tasks, thereby reducing the power consumption of the system further. To do so, we incorporate the memory allocation problem into the problem model of processor's voltage scaling, and evaluate the effectiveness of the combined approach.

***Keywords* — dynamic voltage scaling; hybrid memory; internet-of-things (IoT); non-volatile memory; real-time task scheduling**

I. INTRODUCTION

Due to the recent advances in mobile networks, embedded systems, and sensor technologies, IoT (Internet-of-things) grows rapidly in various application domains such as health care, smart living, national defense, and safety management. IoT is an emerging spotlighted technology that enables the connection of sensor-attached embedded systems such as wearable devices, smartphones, or mobile appliances through wired/wireless networks. IoT devices can be considered as independent systems with separate functions, but they also collect various physical data from sensors and transfer them to other IoT devices and/or cloud servers. Thus, they should satisfy the deadline constraints of legacy real-time systems, and also fulfill the low-power consumption requirement due to battery-based power supplies. Meanwhile, it was recently analyzed that the power consumption of memory subsystems is getting reached to almost 40 % of the total power consumption in mobile systems due to the appearance of memory-intensive applications and increased DRAM capacities [1]. Such tremendous power consumption results mainly from the refresh operation of DRAM [2]. As DRAM is a volatile medium, it requires continuous power recharge in order to retain its data even in idle states.

Recently, non-volatile memory technologies have emerged as an attempt of saving the power consumption in memory subsystems [2]. Non-volatile memory such as PCM (phase-change memory) or STT -MRAM (Spin Transfer Torque Magnetic RAM) stores data without refresh operations because of its non-volatile characteristics. Non-volatile memory has strong merits in low-power consumption, but it also has some weaknesses as a main memory medium; its access time is relatively slower than DRAM and it usually has limited write endurance cycles. For example, PCM is 1-5x and 5-25x slower than DRAM in read and write operations, respectively, and it has the limited endurance of 10^6 to 10^8. Although non-volatile memory is not appropriate for the sole memory medium of a system, it can be used as an auxiliary memory likely to be used along with DRAM for the purpose of power-saving [2], [3].

Another important technique that can be utilized for power-savings in IoT devices is dynamic voltage scaling. With an incredibly enhanced performance of processors during the last a few decades, dynamic voltage/frequency scaling techniques have been widely used in real-time task scheduling [4], [5], [6], [7].The main purpose of voltage scaling, which is based on CMOS digital circuit technologies, is to manage the power consumption of a processor by lowering the supplied voltage of the processor, resulting in low clock frequency. Although the execution time will be increased due to the lowered processor's frequency, power consumption in CMOS digital circuits is proportional to the square of the supplied voltage [6], [7], and thus lowering voltage/frequency leads to the reduction of the processor' power consumption. Based on this, when the load of tasks is lower than the processor's full capacity, dynamic voltage scaling is effective in saving power consumption without sacrificing the deadline constraints of real-time tasks.

TABLE 1. MEMORY ACCESS LATENCIES AND POWER CONSUMPTION

	DRAM	PCM
Read latency	50 (ns)	100 (ns)
Write latency	50 (ns)	350 (ns)
Read energy	0.1 (nJ/bit)	0.2 (nJ/bit)
Write energy	0.1 (nJ/bit)	1.0 (nJ/bit)
Idle power	1 (W/GB)	0.1 (W/GB)

In this paper, we show that power consumption of real-time embedded systems can be further reduced by combining voltage/frequency scaling techniques with task allocation in hybrid memory. If a task set is schedulable in a low voltage mode of a processor, it is still likely to be schedulable even though we use slow memory for that task set. Our intention is to allocate tasks in non-volatile memory if it does not miss the deadline constraint of real-time tasks, thereby reducing the power consumption of the system further [8], [9]. To do so, we incorporate the memory allocation problem into the problem model of processor's voltage scaling, and evaluate the effectiveness of this combined approach. Simulation experiments show that our technique can reduce the power consumption of IoT devices by 36% on average.

The remainder of this paper is organized as follows. Section II briefly describes the background of this research. In Section III, we describe the system model and the proposed approach in terms of processor voltage scaling and hybrid memory allocation. In Section IV, we show the results of our simulation experiments and discuss them. Finally, we conclude this paper in Section V.

II. BACKGROUNDS

2.1 Non-volatile Memory Technologies

In this section, we briefly describe the characteristics of two well-known non-volatile memory technologies, PCM (phase-change memory) and STT-MRAM (Spin Transfer Torque Magnetic RAM).

PCM stores data by utilizing a material called GST, which is a chalcogenide alloy of germanium, antimony, and tellurium. GST has two different states called amorphous and crystalline. These two states can be set by varying the heating time and temperature. As each state provides different resistance when the electric current is passed, data can be differentiated by reading the resistance on the cell. Whereas detecting the resistive value on the cell is fast, changing the state in a cell takes much time, and thus a write operation is slower than a read operation. Moreover, the number of write operations allowed for each PCM cell is limited to 10^6–10^8. As this is not enough for PCM to be used as main memory, using PCM along with DRAM has been attempted [10]. Also, wear-leveling techniques for PCM have been extensively studied [10].

Though PCM has aforementioned weaknesses to become a main memory medium, it has two strong points regarding low-power consumption and high density. Due to its non-volatile characteristics, PCM does not need refresh operations. This leads to extremely low power consumption during idle time. Another merit of PCM is that it allows higher density than DRAM. In particular, DRAM is hard to fabricate beyond 20 nm. Due to this reason, the recently produced 3D-DDR3 DRAM attempts to scale the capacity by leveraging the 3D stacking technology rather than scaling down the chip size [11],In contrast, it is expected that PCM will have stable characteristics in 5 nm node [13].

In addition to the advances in micro-fabrication processes, multi-level cell (MLC) technologies are also accelerating the density improvement of PCM. Although most PCM prototypes are being produced as a single-level cell (SLC), which considers only the two states of crystalline and amorphous, recent research has demonstrated that additional intermediate states can be represented. This implies that MLC PCM, which allows for storing multiple bits in a cell by choosing multi-levels of electrical charge, will be possible [15]. Due to this reason, PCM would have an order of magnitude higher density than other non-volatile memory media, such as FeRAM (ferroelectric RAM) and MRAM (magnetic RAM), that are structurally hard to provide MLC. Thus, major semiconductor manufacturers, including Samsung and Intel, are now preparing for the commercialization of PCM technologies.

STT-MRAM is another promising non-volatile memory technology. STT-MRAM is based on magnetic properties of material whose magnetic orientation can be controlled and sensed using electrical signals. Specifically, STT-MRAM uses a Magnetic Tunneling Junction (MTJ) device to store data [14]. Data in an MTJ, which consists of two ferromagnetic layers and one tunnel barrier layer, is represented by a resistance value that varies based on the relative magnetization directions of the two ferromagnetic layers [16]. When the magnetic field of the two layers are parallel (i.e., aligned in the same direction), the MTJ resistance is low, and this represents a logical zero. When the two layers are anti-parallel to each other (i.e., aligned in the opposite direction), the MTJ resistance is high, and this represents a logical one.

To read data stored in a cell, a small voltage needs to be applied between sense and bit lines, and the amount of current flow is sensed. To write to an STT-RAM cell, a large current needs to be pushed through the MTJ to change the magnetic orientation. Depending on the direction of the current, the two ferromagnetic layers become parallel or anti-parallel. The amount of current required for writing into an MTJ is significantly larger than that needed for reading from it.

2.2. Low-Power Techniques for Real-time Task Scheduling

A lot of studies have been performed to reduce the power consumption of real-time systems using dynamic voltage scaling [4], [5], [17], [18].

Pillai and Shin propose a mechanism of selecting the lowest possible operating frequency that will meet all deadlines for a given task set [7]. They addressed three algorithms for dynamic voltage scaling: static voltage scaling, cycle-conserving voltage scaling, and look-ahead voltage scaling. Static voltage scaling selects the voltage of a processor statically whereas cycle-conserving voltage scaling utilizes reclaimed cycles for lowering the voltage when a task does not spend its full worst case execution time. Look-ahead voltage scaling lowers the voltage further by determining future computation requirements and deferring the execution of the task in accordance.

Ghor and Aggoune aim at finding the least energy voltage schedule for real-time tasks using dynamic voltage scaling [5]. To reduce processor energy, a slack-based method is used, which stretches the task execution time whose length is identified through off-line computing and schedules as late as possible without missing deadlines.

Lee et al. also use slack times to lower the processor's voltage/frequency [6]. In their scheduling, voltage setting assigned to each task at initial time is dynamically switched upon reclaiming the unused clock cycle when a task completes the execution ahead of the worst case execution time.

Lin et al. point out that there is a memory mapping problem caused by different worst case execution time as heterogeneous memory types are used [8]. They use dynamic programming and greedy approximation for solving memory allocation problems without violating deadline constraints.

Zhang et al. propose task scheduling and allocation schemes for hybrid memory architectures to save energy consumption without violating deadline constraints [19]. In their scheme, tasks are allocated one by one to non-volatile memory and the schedulability of the task set is checked. This procedure is repeated until all tasks are examined. They also use the reclaimed slack time for the ready tasks to be executed partially on low power non-volatile memory.

III.COMBINING PROCESSOR VOLTAGE SCALING AND MEMORY TASK ALLOCATION

3.1. System Model

Let $\Gamma = \{ \tau 1, \tau 2, \ldots, \tau n\}$ be the set of n independent tasks in a real-time system, which has a processor capable of dynamic voltage/frequency scaling, and main memory consisting of DRAM and non-volatile memory. Each task τi is characterized by a tuple $<Ci, Ti, Mi>$ where Ci is the worst case execution of τi, Ti is the period of τi, and Mi is the memory footprint of τi . In our task model, each period of a task implicitly represents the deadline of the task.

A processor is assumed to be operated at two different voltage modes: default mode and low-power mode. Suppose that the voltage values of the default mode and the low-power mode are VD and VL, respectively. Then, the corresponding clock frequency for these two modes can be defined as fD and fL, respectively, such that $fD > fL$.

When a processor operates in a low-power mode, the execution time becomes longer than in the default mode due to the lowered clock frequency. Nevertheless, it would spend less power as the power consumption is proportional to the square of the supplied voltage. As the worst case execution time of a task is defined based on the default mode of a processor, it will be lengthened to $(fD / fL) \cdot Ci$ when the processor changes its state to a low-power mode. Meanwhile, it is known that EDF (Earliest Deadline First) is an optimal scheduling algorithm in real-time task scheduling [20], [21]. Optimality here implies that no other algorithm can schedule a task set if we cannot find a feasible schedule for that task set with EDF. Based on this, EDF is used as a default real-time task scheduling algorithm in this paper. Note that EDF schedules a task with the closest deadline first in the task set.

The schedulability of a real-time task set Γ can be tested by the utilization U of a processor as follows.

$$U = \sum_{i=1}^{n} \frac{C_i}{T_i} \le 1 \qquad (1)$$

If a processor is executed in a low-power mode, the worst case execution time Ci of a task τi will be adjusted accordingly, and thus the processor's utilization U needs to be tested with the new Ci values. We extend our model to redefine the worst case execution time of a task by considering the memory types of tasks allocated. That is, as the access latency of non-volatile memory is longer than that of DRAM, a task allocated to non-volatile memory will need more time to be executed. Our extended model redefines the worst case execution time of a task whose memory access time depends on different memory types as well as the delays that occur due to the processor's voltage scaling. Accordingly, a task set Γ is divided into two subsets of ΓL, a subset of tasks allocated to non-volatile memory, and ΓD, a subset of tasks allocated to DRAM, such that $\Gamma = \Gamma L * \Gamma D$, which are determined by the memory types each task assigned. The worst case execution time of tasks in each subset is redefined appropriately.

By considering some common assumptions used in previous studies [6], we maintain five assumptions for our system model.

A1. The size of DRAM is large enough to accommodate entire task sets, but the power is turned off for the part of DRAM the tasks are not allocated to.

A2. Once a task is allocated to either DRAM or non-volatile memory, it is not allowed for the task to migrate between the two memory types during its execution.

A3. Each task is executed independently and does not affect other tasks.

A4. Context switch overhead, i.e. overhead of switching a processor from one task to another, and voltage switching overhead, i.e. overhead of switching a processor between a low-power mode and the default mode, are negligible.

A5. Frequency of a processor is set to an appropriate level as the voltage supply is adjusted.

3.2. Dynamic Voltage Scaling in Real-Time Task Scheduling

In general, offline scheduling is possible for a real-time task set released periodically. For example, let us see the scheduling results with EDF for the task set listed in Table 2. The schedulability of the task set is tested by calculating the utilization of the tasks τ1, τ2, and τ3, and adding up them i.e., *U*

= 2/8 + 1/10 + 1/14 = 0.421. As the total utilization is less than 1, the task set is schedulable under the EDF algorithm. Figure 1 shows the scheduling result for the task set given in Table 2

TABLE 2. AN EXAMPLE OF A TASK SET

Task	Worst case execution time	Period
τ_1	2	8
τ2	1	10
τ3	1	14

Fig. 1. A scheduled task set without voltage scaling.

with EDF. Tasks τ1, τ2, and τ3 are all ready to be executed when the time *t*=0. Of these, task τ1 is first selected and executed as its deadline is the closest. Then, task τ2 is subsequently selected for execution as the time *t* becomes 2. Task τ3 is, then, selected and executed at time *t*=3. After that, the next period of the tasks arrives and they will be executed again. For example, task τ1 is scheduled again at time *t*=8, and other tasks will also be scheduled subsequently as their next periods arrive.

Although the task set is schedulable, idle intervals, such as (4, 8), (11, 14), (15, 16), and (18, 20) occur frequently, which reach up to 50% of the total possible working time of the processor. To relieve this inefficiency, we lower the processor’s voltage/frequency for some idle intervals. For example, if two low voltage/frequency levels of 0.25 and 0.5 are applied for tasks $\tau2$ and $\tau3$, respectively, the worst case execution time of $\tau2$ and $\tau3$ will be lengthened to 4 and 2, respectively, for the same example in Table 2. Accordingly, the utilization of the processor is increased to $U = 2/8 + 4/10 + 2/14 = 0.793$, which is still less than 1 and thus schedulable with EDF. Figure 2 shows the scheduling result of EDF when the aforementioned voltage scaling is adopted. As we see, idle intervals are decreased significantly when compared with the original scheduling result in Figure 1, which leads to the reduction of processor’s power consumption.

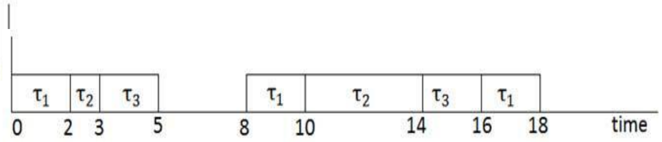


Fig. 2. A scheduled task set with dynamic voltage scaling.

3.3. Real-time Task Allocation on Hybrid Memory

Non-volatile memory like PCM is slower than DRAM in its access latency, but consumes less energy as it requires no refresh power. To further reduce the power consumption of real-time systems, this paper combines dynamic voltage scaling and memory allocation on hybrid memory consisting of DRAM and non-volatile memory as shown in Figure 3.

As the worst case execution time of a task is defined as the longest time of the possible memory paths for the task to be executed, i.e. time to access DRAM due to a miss from the on-chip cache memory. Thus, in hybrid memory systems, if a task

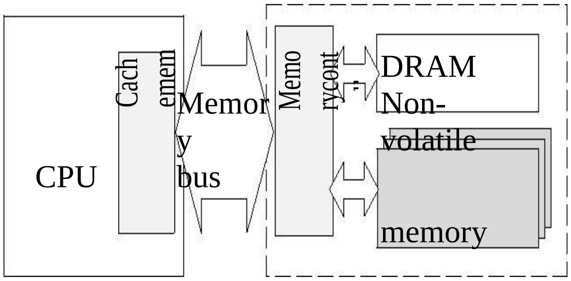


Fig. 3. System architecture of the proposed system

resides in non-volatile memory rather than DRAM, the worst case execution time of the task should be redefined by considering the increased access latency of the non-volatile memory.

Our extended task model reflects the existence of non-volatile memory, thereby defining the worst case execution time of a task considering non-volatile memory as well as dynamic voltage scaling. Specifically, we tightly model the worst case execution time of a task considering the overlapped time components between processor and memory (e.g., cache memory and pipelining). Accordingly, when the schedulability test is performed for the EDF algorithm, the processor's utilization is calculated by the worst case execution time defined tightly according to our extended task model.

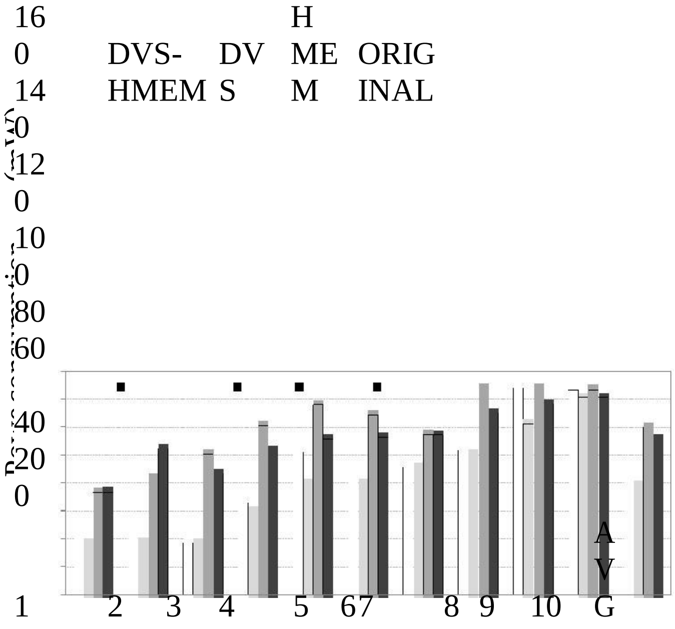
In reality, a lot of research has been performed on processor's voltage scaling in task scheduling and hybrid memory based task allocation. However, the two approaches are independently studied and their effectiveness is not investigated altogether. Our contribution is that we quantify the relative effectiveness of the two approaches and combine them for maximizing the energy-savings of real-time embedded systems.

IV. PERFORMANCE EVALUATIONS

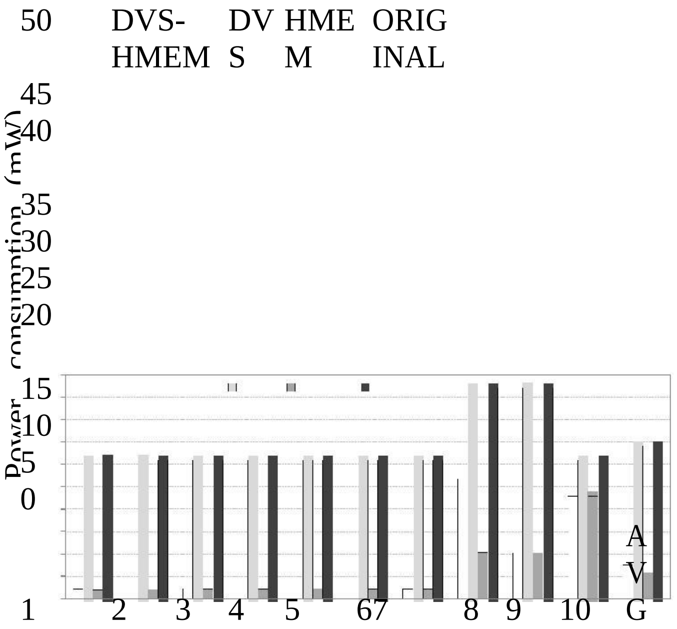
In this section, we analyze the performance evaluation results of simulation experiments executed to assess the effectiveness of the proposed technique. Similar to previous studies [8], we create 10 task sets varying the load of tasks for a given processor capacity. We compare our technique called DVS-HMEM (dynamic voltage scaling with hybrid memory allocation) with DVS (dynamic voltage scaling) that uses processor voltage scaling but does not use hybrid memory allocation, HMEM (hybrid memory allocation) that uses hybrid memory allocation without processor voltage scaling, and ORIGINAL that does not adopt either dynamic voltage scaling or hybrid memory allocation.

The sizes of DRAM and non-volatile memory are equally set to accommodate the entire task set and the access latency and the power consumption of the two memory media are set as listed in Table 1. We use two voltage/frequency modes of a processor: the default mode of 1.0 and the low-power mode of 0.5.

Figures 4(a) and 4(b) show the power consumption in processor and memory, respectively, for the four schemes aforementioned as the task sets are varied. As shown in Figure 4(a), DVS and DVS-HMEM, which adopt dynamic voltage



Task set
(a) Power consumption in processor



Task set

(b) Power consumption in memory

Fig. 4 Comparison of power consumptions for each technique.

scaling, similarly save a substantial amount of processor's power consumption. HMEM and ORIGINAL, which do not use voltage scaling, show relatively higher energy consumption than DVS and DVS-HMEM, although the gap becomes small in some cases like task set 10. In particular, processor's voltage scaling is less effective as the task set's load approaches the full capacity of a processor. This is because the chance of utilizing idle periods of a processor becomes difficult by voltage scaling in such cases. Note that the load of a task set becomes heavy as the task set number increases in our cases.

Figure 4(b) shows the power consumption in memory for the four techniques as the task sets are varied. As shown in the figure, DVS-HMEM and HMEM, which use non-volatile memory along with DRAM for task allocation, consume significantly less energy than DVS and ORIGINAL that only use DRAM. This is because idle power of non-volatile memory is close to zero, and thus the reduced size of DRAM used due to adopting non-volatile memory significantly saves the refresh power of DRAM.

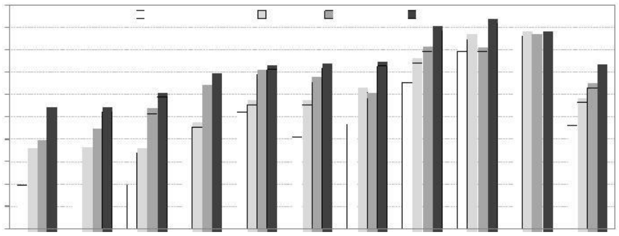
However, as the access latency of non-volatile memory is longer than that of DRAM, executing a task in non-volatile memory may increase the execution time in the processor, possibly leading to increased processor's power consumption. However, as shown in Figure 4(a), such a phenomenon happens only in HMEM and it disappears in DVS-HMEM that uses processor voltage scaling along with non-volatile memory allocation.

When comparing the results of DVS and DVS-HMEM, we can see that adopting non-volatile memory does not increase the processor's power consumption if the processor adopts dynamic voltage scaling. This is because power-savings can be maximized by executing a task in a processor's low-power mode when the task is allocated on slow non-volatile memory.

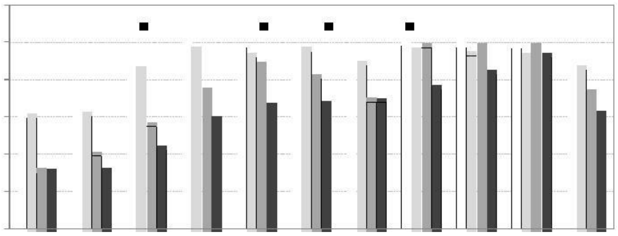
Figure 5 shows the total energy consumption of the system by adding up the consumed energy in processor and memory. As shown in the figure, DVS-HMEM saves the energy consumption of ORIGINAL, DVS, and HMEM, respectively, by 36%, 18%, and 28% on average. Figure 6 shows how the processor's utilization changes as we use dynamic voltage scaling, hybrid memory allocation, and combining the two techniques. As we see, the proposed DVS-HMEM shows the highest processor utilization in all cases, and the utilization is close to 100% in some cases.

V. CONCLUSION

In this paper, we showed that the power consumption of real-time embedded systems can be reduced by combining processor's voltage/frequency scaling techniques with task allocation in hybrid memory. This is based on the synergy effect of the processor's voltage scaling and the hybrid memory allocation. That is, if a task set is schedulable in the low-power mode of a processor, it is still likely to be schedulable even though we use slow memory for that task set. By considering this, we adopt non-volatile memory technologies that consume less power than DRAM but provide relatively slow access latency. Specifically, we incorporate the memory allocation problem into the problem model of the processor voltage scaling, and evaluate the effectiveness of the combined approach. Experimental results have shown that the proposed technique reduces the power consumption of real-time systems by 36% on average.



Task set Fig. 5 Comparison of total power consumption.



Task set Fig. 6 Comparison of processor utilization.

REFERENCES

[1] A. Carroll and G. Heiser, "An Analysis of Power Consumption in a Smartphone," Proc. USENIX Annual Technical Conf., 2010.

[2] S. Lee, H. Bahn, and S. H. Noh, "CLOCK-DWF: A Write-History-Aware Page Replacement Algorithm for Hybrid PCM and DRAM Memory Architectures," IEEE Trans. Computers, Vol. 63, No. 9, pp. 2187-2200, 2014.

[3] E. Lee, H. Bahn, and S. H. Noh, "Unioning of the Buffer Cache and Journaling Layers with Non-volatile Memory," Proc. USENIX Conf. File and Storage Technologies, pp.73-80, 2013.

[4] K. Choi, W. Lee, R. Soma, and M. Pedram, "Dynamic Voltage and Frequency Scaling Under a Precise Energy Model Considering Variable and Fixed Components of the System Power Dissipation," Proc. IEEE Int'l Conf. Computer Aided Design, pp. 29-34, 2005.

[5] H.E. Ghor and E.M. Aggoune, "Energy Saving EDF Scheduling for Wireless Sensors on Variable Voltage Processors," Journal of Advanced Computer Science and Applications, Vol 5, No. 2, pp. 158-167, 2014.

[6] Y. Lee, Y. Doh, and C. Krishna, "EDF Scheduling Using Two-Mode Voltage Clock Scaling for Hard Real-Time Suystems," Proc. ACM CASES Conf., pp. 221-228, 2001.

[7] P. Pillai and K.G. Shin, "Real-Time Dynamic Voltage Scaling for Low-Power Embedded Operating Systems," Proc. ACM Symp. Operating Systems Principles, pp. 89-102, 2001.

[8] Y. Lin, N. Guan, and Q. Deng, "Allocation and Scheduling of Real-Time Tasks with Volatile/Non-Volatile Hybrid Memory Systems," Proc. IEEE Non-Volatile Memory System and Applications Symposium, pp. 1-6, 2015.

Automated vehicular system based on inter vehicle communication

[1]M. DHIVYA, 2V. SURYA, [3]P. KOWSALYA
UG Students
AKT MCET
[1]Dhivya2911md@gmail.com, [2]surya1996as@gmail.com

Abstract:

Nowadays vehicular traffic is a major problem. Drivers choose the route that they believe will be the fastest; however, traffic congestion can significantly change the duration of a trip. Providing real-time traffic information to drivers and navigation systems helps them to choose the best route. In this paper, we first establish a hybrid intelligent transportation system (ITS), i.e., a hybrid-VANET-enhanced ITS, which utilizes both vehicular ad hoc networks (VANETs) and cellular systems of the public transportation system to enable real-time communications among vehicles, roadside units (RSUs), and a vehicle-traffic server in an efficient way. Also proposed Path planning algorithm, it is based on the hybrid ITS framework, a multi hop message forwarding mechanism is designed to collect the real-time traffic information or the emergent warning messages, which usually have strict delay bounds.

Keywords: Vehicular Ad – hoc Network (VANET), ITS, RSU.

I. INTRODUCTION

Advanced in wireless communication technology leads to the number of applications area. Recently ad hoc networks or wireless ad hoc networks are emerging wireless communication technologies. It includes 2 different types of communication modules i.e. Mobile ad-hoc network (MANET) and Vehicular ad-hoc network (VANET). VANET is a sub section of MANET used to give an efficient communication between the movable nodes. Recently wireless communication getting an immense significance in vehicular equipment to provides efficient information about the path information, traffic density in particular path etc between the nodes. VANET is a low range communication technology, USA‘s Federal Communication Commission standardize the 75MHz function bandwidth in 5.9GHz band [01].

Typical VANET communication network involved 2 different types of communication methods

1. Vehicle – to – Vehicle (V2V) Communication.
2. Vehicle – to – Infrastructure (V2I) Communication.

VANET is completely infrastructure less. This is characteristic make VANET communication technologies more complex. The other most important parameter which makes the VANET communication most challenging is listed as

- The surrounding Vehicle environmental condition (i.e. Reflective surface).
- The dynamic speed of vehicles will affect the radio communication.
- Frequency interference of 2 different movable nodes.

. The sample of VANET with both V (vehicle) to V and V (vehicle) two I is presented in Figure 1. As previously mentioned routing is method of challenging and significance operations of VANET. In which data can be sending from source to destination node either by using multi hop. Routing protocols are used for the system performance is analyzed by using some significance technical parameters i.e. latency, operational frequency range. These parameters are reached up to the reasonable values and in certain outline the level of packet loss is almost minimized.

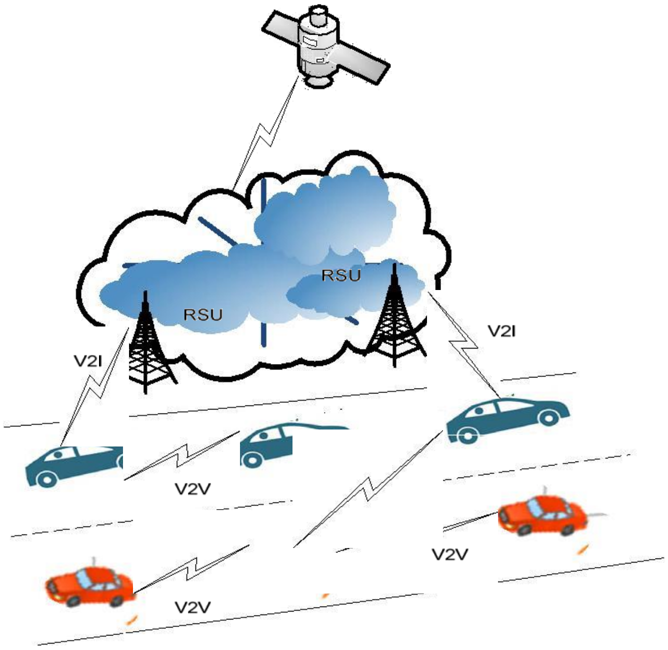


Figure 1: Sample of VANET

Since from few decade lot of research is conducted on VANET and its routing protocols. The survey of little research work is given in below section. Further in proposed paper the designer mainly concentrated on location based routing communication. The designing of system and its functioning is briefly explained in methodology section.

II. LITERATURE SURVEY

Ye Tao et.al [03] has designed location based routing protocol in VANET, in which they mainly concentrated on duplication of packet and encapsulation. Topology is significant functional characteristics of VANET. Sudden change in the topologies will lead to the loss in the packet network. In the referred paper author is mainly concentrated on this problem. Geo-Networking standard networking infrastructures used to reduce the losses in packet problem. Both routing challenges and routing encapsulation difficulties are reducing by the application of Duplicated Unicast Packet Encapsulation (DUPE) protocols. The cluster will be the cluster lead. While passing the node information it must be necessary to keep the zone construction and the numbering of sequences of each vehicle in the cluster. The application of moving zone based routing protocol presents a better packet transmission rate and minimize the complexity overhead involved during data communication.

Nikolaos Mantas et.al [08] designed a VANET system module, mainly concentrated on finding the misbehavior of the node. The module is implemented by using Cross Layer, Weighted, Position based Routing protocols (CLWPR). In the referred paper it assumed that few of the nodes which purposefully drop the packets in the network i.e. before researching to the final position. The application of CLWPR location based routing algorithm increase the system aspects to meet the requirement during data communication. The performance of the designed module measured w.r. to the packet receive ratio. The application of CLWPR position based routing protocol efficiently increase the packet receive ratio up to by 30%.

Vehicular Ad hoc network is very challenging concepts and finding optimal path of each node is much more difficult due its functional characteristics. Guangyu Li et.al

[9] has designed an Ant Colony Optimization (ACO) based vehicular Ad hoc Network. Due to the characteristics of network i.e. large operating range, speed of vehicular system and rapid change in the network topology increases the difficulty of implementing an efficient Vehicular Ad hoc Network. In the referred paper system designer proposes an AQRV (Adaptive Quality of Service) based data routing protocols. While passing the packets from starting point to destination, the application of routing algorithm efficiently select the optimal path which meets the Quality of Service (QoS) condition. In the referred paper the system performance i.e. QoS is measured in terms of packet delay, packet delivery ratio and node connectivity. The routing selection is mathematically computed and optimization challenges are overcome by using ACO algorithm. Along with the ACO algorithm a Local QoS Models (LQM) is proposed and integrated to join the best QoS for urban vehicular ad hoc network.

The literature survey reveals that most of the research work is done on both clustering and non clustering based vehicle to vehicle communication but none of the work is union with moving objects in V2V communication. The limitation involved in V2V communication specially with moving object is overcome by application moving object zone based routing protocol. The system architecture, working flow and routing finding methods are presented in below section.

III. METHODOLOGY

The design an inter vehicle communication module there must be necessary to analyze the environmental attribute of the node. In every environmental condition vehicle has its own characteristics. Before designing any VANET intercommunication module there must be a necessary to have the knowledge about the characteristics of each node in that particular environmental condition. The random nature of the vehicle i.e. it changes its position randomly, the velocity is going to be changes and obliviously direction is not at all fixed. These characteristics of vehicle increase the level of complexity, vehicle collision is the common and dangerous thing happen in the vehicular movements. This can be prevented or eliminated by calculating the optimal position of each node in a geographical area. The proposed moving object zone based routing system architecture flow in Figure 5.

The architecture is purely providing vehicle-to-vehicle communication. A self formed moving object zone is created to give an extensive routing solution of VANET. The above architecture pictorially explains the concepts of our proposed work. In which moving zones are presented by cloud symbol and propagation connectivity is shown by the arrows. The purpose of the designed system is to combine the functional parameter of moving objects and rule them by providing an effective vehicle management. The location of the moving object is collected from GPSR.

It is always in three dimensional space i.e. 'r' is radial distance, θ (theta) polar angle and lastly azimuthal angle is denoted by φ (phi). By using spherical co-ordinate system these values are converted into an x, y and z plane. In which it is assumed that z plane is considered as 0. Based on x and y axes plane a correct position of the node is estimated. The pictorial representation of X and Y axis estimation is shown in below Figure 2. This position information about the vehicular node is applied for routing the data between the movable vehicles.

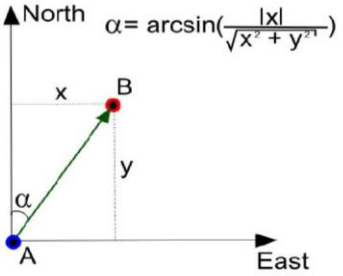


Figure 2: X and Y Distance Computation

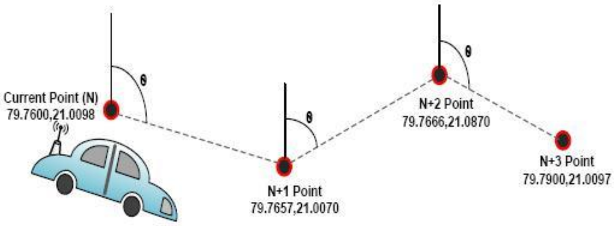


Figure 3: Sample Module of X and Y axis of Movable Vehicle

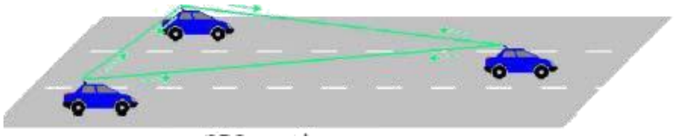


Figure 4: Integration Between Vehicle within a Zone

In the proposed work a respective zone or functional range of each node is estimated based their moving patterns (i.e. Speed, direction and distance). After collecting the proper position details of each node, the movement information is continuously updated in the index of the node storage and vehicle management. The pictorial representation of vehicle X and Y axis and the interrelation between them are shown in Figure 3 and Figure 4.

It presents the reasonable clustered based approach, in which depending on the moving patterns vehicles are grouped. Each moveable node continuously update it information along with that node head is able to finding the current position of the adjacent node by using index information. The use of index information efficiently reduces the network overhead involved in position estimation of each network, path estimation and delay in packet delivery. The working of proposed routing algorithm, zone formation and vehicle - to – vehicle communication

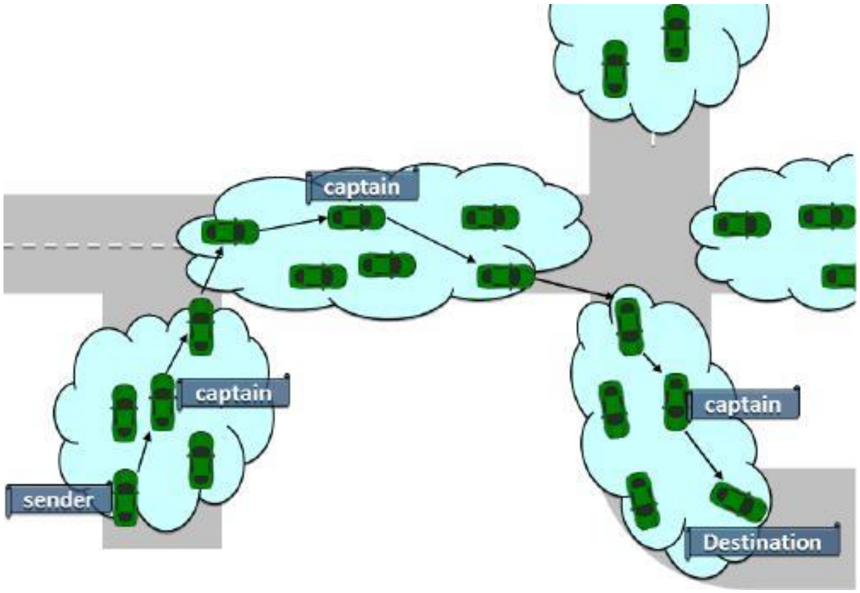
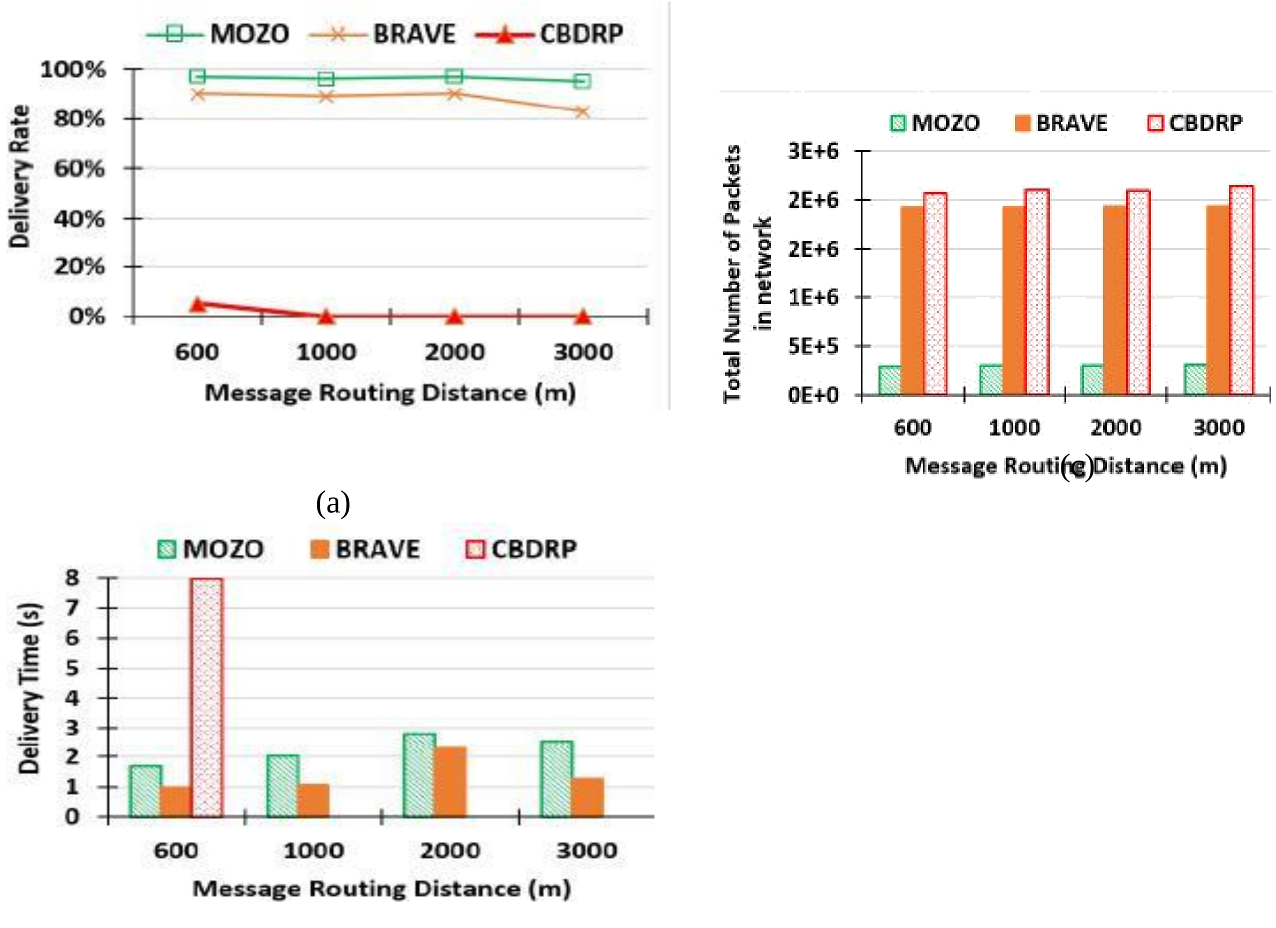


Figure 5: Proposed System Operational Block Diagram

IV. EXPERIMENTAL RESULT

A network is initialized with 10 random movables nodes. The distance between the nodes is varied (i.e. from 600 to 3000 meters) to estimate system response for fixed number of data packets. Initially each node broadcast a beacon messages to collect nearest neighbor node information and these beacon messages are retransmitted in every 2s. For each distance a 90 messages are transmitted between the two nodes. The performance of the Mozo (Moving object zone routing protocol is compared other two VANET routing protocol i.e. BRAVE (Beacon less Routing Algorithm for Vehicular Environment) and CBDRP (Clustering Based Directional Routing Protocol). Depending packet delivery rate and transmission time is proved that proposed system presents highest packet delivery rate. The graphical analysis packet delivery rate, packet delivery time and number of packets in the network is presented in below Figure 7. (a), (b) and (c).

The performance of system is also evaluated with and without traffic controls. From the performance analysis it is proved that proposed moving object zone protocol present the reliable output.



(c)

(a)

(b)

Figure 7: (a) Delivery Rate; (b) Delivery Time; (c) Total Number of Packets

V. CONCLUSION.

The safety level of persos life at urban and highways increases by the application or designing of efficient VANET network. The integration of GPS information. In which each node actively communicates with the adjacent node by which come under the. From the simulation result it is proved that designing a VANET by using RSU based routing protocol effectively enhance the system performance in tem of increasing the packet delivery ration and reducing packet delay time between vehicle to vehicle communications. The RSU is used as a mediator for authentication of both the RSU and the requesting vehicle.

REFERENCES

[1] Yun –Wei Lin, Yuh – Shyan Chen and Sing – Ling Lee, "Routing Protocols in Vehicular Ad Hoc The safety level of person‟s life at urban and highways increases by the application or designing of efficient VANET network. The integration of GPS information, spherical ordinates and MoZo routing protocol effectively identifies the nearest node within the predefined clustered zones. In which each node actively communicates with the adjacent node by which come under the. From the simulation result it is proved that designing a VANET by using Moving Zone based routing protocol effectively enhance the system performance in tem of increasing the packet delivery ration and reducing packet delay time between vehicle to vehicle communications. Network: A Survey and Future Perspectives", Journal of Information Science and Engineering, V0l. 26, pp. 913-932, 2010.

[2] Prabhakar Ranjan, Kamal kant Ahirwar, "Comparative Study of VANET and MANET Routing Protocols", International Conference on Advanced Computing and Communication Technologies, 2011.

[3] Ye Tao, Xin Li, Manabu Tsukada and Hiroshi Esaki, "DUPE: Duplicated Unicast Packet Encapsulation in Position-Based Routing VANET", IEEE, pp. 123 -130, 2016.

[4] Mayank Bhatt, Shabnam Sharma, Aditya Prakash, Dr. U.S.Pandey and Dr. Kiran Jyoti, "Traffic Collision Avoidance in VANET Using Computational Intelligence", International Journal of Engineering and Technology, 2016.

[5] Qing Ding, Bo Sun, Xinming Zhang, "A Traffic-light-aware Routing Protocol based on Street Connectivity for Urban Vehicular Ad hoc Networks", IEEE, Vol. 20, Issue 8, pp. 1635 – 1638, 2016.

[6] A. M. Oranj, R. M. Alguliev, Farhad Yusifov and Shahram Jamali, "Routing Algorithm for Vehicular Ad Hoc Network Based on Dynamic Ant Colony Optimization", International Journal of Electronics and Electrical Engineering, Vol. 4, No 1, 2016.

[7] Dan Lin, Jian Kang, Anna Squicciarini, Yingjie Wu, Sashi Gurung, and Ozan Tonguz, "MoZo: A Moving Zone Based Routing Protocol Using Pure V2V Communication in VANETs", IEEE, Vol. 16, Issue 5, pp. 1357-1370, 2017.

[8] Nikolaos Mantas, Malamati Louta, Konstantinos Katsaros and Stylianos Kraounakis, "Social CLWPR: A Socially Enhanced Position Based Routing Protocol for Handling Misbehavior in VANETs", IISA, 2017.

Smart Health Management Based on IoT

Mrs.M.Phemina Selvi
Assistant Professor, Dept. of Electronics and
Communication Engineering,
University College of Engineering Villupuram
Villupuram, Tamil Nadu.
vm.femina@gmail.com

Manimegalai Arunachalam, Z.S.Subhashini, Ezhilarasi Pavadai,UG student
Dept. of Electronics and Communication Engineering,
University College of Engineering Villupuram
Villupuram, Tamil Nadu.
aa.manimegalai@gmail.com
Subashinisaravanan05@gmail.com

***Abstract*— Variety of appliances have been presented in a house with the development of social economy and rapid increase in the needs of the people. There is a problem in the management and control of these appliances so as to meet the comfort, health and security at Room. To overcome this problem a smart control based system has been proposed. When we talk about Internet of Things (IoT), there are large numbers of distinct devices which are connected throughout different systems. These systems provide open platform to all digital devices accessing data from such systems. So, it becomes quite difficult to design such a system for IoT which can handle large classification of devices and also technologies like link layer associated to it. To connect such a sophisticated network on IoT one need to have central server (server could be created over Wi-Fi network) which can facilitate all smart phones, tablets and other digital devices.**

Keywords: IoT, AT mega controllers, Sensors, Wi-Fi shield, Relay

I.INTRODUCTION

It is inevitable that Internet has become one of the important parts of our daily life. The new mega trend of Internet is Internet of Things (IOT). A world where several objects can sense, communicate and share information over a Private Internet Protocol (IP) or Public Networks through visualizing Manner. The interconnected objects collect the data at regular intervals, analyze and used to communicate between objects and initiate required action for control of those objects or remote monitoring. This method include embedded technology which allows them to exchange information, with each other or the Internet and it will be assess that about 8 to 50 billion devices will be connected by 2020. The entire concept of IOT stands on sensors, gateway and wireless network which enable users to communicate and access the application/information. Among all the regions no place does the IOT offer more prominent guarantee than in the field of health awareness and the Room Management. As saying "Health is wealth" and "saving Electricity" it is considered to be a great advantage. This IOT framework which gives secure health awareness checking and also to conserve the Electricity. So outlining a framework where client information is gotten by the sensor and sent to the cloud through Wi-Fi and permitting just approved clients to get to the information.

II INTERNET OF THINGS

The IOT is usually consider as connecting things to the Internet and using that connection for control of individuals objects otherwise remote monitoring. The products urbanized based on IOT include embedded technology which allow them to exchange information, through each additional the Internet and it is assess that about 8 to 50 billion devices will be connected by 2020 because these devices come online, they provide improved life style, construct safer and more engaged communities in addition to revolutionized healthcare. It’s just one more computer right all of the same issue we have with access control, vulnerability management, patching, monitoring, etc. Envision your network with 1,000,000 more devices.

III. RELATED WORKS

In recent years, the IoT has become a hot topic of global Concern, which provides a new direction to the indoor Environment intelligent detection and control system. At present, remote monitoring and control for indoor environment by using the embedded technology combination of wireless sensor network to construct Internet of Things has become the development trend and research focus in the smart home[1-3].And many scholars has great contributions to the indoor environment function detection and control system which help our design much.

A. Intelligent Building Developed Model

Szász proposed the basic concept of intelligent building – a combination of technology and processing that makes residents feel more comfortable, safe and efficient construction, and leads to four original intelligent building development model: residents, information, energy and adaptation (IIEA)[4]. In order to manage and control intelligent buildings better, Yinbo Wu designed a web-based integration model which is independent of platform, protocol and language, and can achieve remote control [5]. On the basis of intelligent building, Nian Xue, put forward a secure SDN framework named as S 2 Net, and designed a variety of security protocols to ensure the release and exchange of informations [6].

B. Intelligent Management System Prototype Design

Azka Ihsan Nurrahman and Kusprasapta Mutijarsa put forward four levels of intelligent management system: physical layer, communication layer, data processing layer and application layer, and they also proposed the required corresponding hardware components at all levels, such as the physical layer requires sensors, microcontrollers, etc. To obtain the original information, the communication layer requires a wireless network for information exchange [7]. Himanshu Verma and others design the HTML Web Page as a software entity, and combine the database to collect and collate the data of the indoor environment, which provides the idea for the prototype design of the indoor environment monitoring and control system [8].

C. Wireless Sensor Networks

In order to improve the accuracy and reliability of the indoor environment inspection and control system, a sensor network can be used to carry out information interaction. Lianjin Guo proposed an integrated detection and control system for embedded and multi-sensors, which are stored and displayed by the remote PC on the data collected by the sensor [9]. Tao Hu proposed a hybrid network program based on ZigBee-based wireless sensor network [10]. It realizes the information exchange between terminal equipment and environmental monitoring equipment through wireless network, and improves the flexibility and convenience of intelligent home system by using mobile terminal remote control system Sex.

D. The Design and Implementation of Smart Home System

Based on IoT Shen Bin proposed an intelligent home model based on the Internet of things. The model detects the indoor environment through various sensors, uses the Zigbee wireless network to access the information gateway gateway, and then forwards the information to the servers in the Internet. Users
can view the information of each subsystem in real time and control the operation of home equipment through a mobile phone or a browser or client software on the computer [11]

IV.PROPOSED SYSTEM

The main idea of this system transmitting the data through the webpage to continuous monitoring of the patients and the state of the room over internet. In this system we used Atmega 328p, act as a gateway that collects the data from the sensors and sends the data through IOT. The Protected data sent can be access anytime by the doctors by typing the corresponding exclusive IP address in any of the Internet Browser at the end user device (ex: Laptop, Desktop, Tablet, Mobile phone). The Atmega is connected to IOT which provides information to doctor/caretaker when the heart rate is greater than 90 or less than 60 and when the room temperature is less than 20 or greater than 35.

In this system, we also introduced glucose level sensor to alert the doctor, since it can prevent the reverse of blood to the strip. And the user interface html webpage will automatically refresh for every 15 seconds for this reason patient health status is continuously send to the doctor. Therefore, continuous monitoring of patient data is achieved.

V. ATMEGA 328P

- Atmega 328p is a single-board Microcontroller.
- It is a gateway to communicate to various sensors.
- Atmega board design use a variety of microprocessors and controllers also equipped with sets of digital and analog (i/o) pins that may be interfaced to various expansion boards and other circuits.

As of 2013 the ATmega328 is commonly used in many projects and autonomous systems where a simple, low-powered, low-cost micro-controller is needed. Perhaps the most common implementation of this chip is on the popular Arduino chip.

HEART BEAT SENSOR

It uses Bright infrared (IR) LED and a phototransistor to detect the pulse of the finger, a red LED flashes with each pulse.

This digital output can be connected to Atmega directly to measure the Beats Per Minute (BPM) rate. It works on the principle of Light modulation by blood flow through finger at each pulse.

- Heart beat indication by LED
- Instant output digital signal for directly connecting to Atmega.
- Compact Size

This sensor has transmitter, receiver and comparator. It works based on the comparison with reference voltage which can be done through comparator circuit. Required voltage: 5V

VI CONCLUSION

When various appliances would be connected over the internet with facility of being switched on and off through a common network system/server and also status about the device is being shared throughout the network then new revolution would be in the world of the internet. Short and basic controlling of appliances is modeled.

VII FUTURE SCOPE

More advancement in this work could be achieved with replacement of Raspberry pi boards in place of Wi-Fi shields. Another aspect that can be added here is that we can interact some sensors through which switching of devices takes place based upon some condition and more accuracy in the system could be achieved. For this work we have made best efforts to understand the controlling of appliances over the internet and makes our homes really smart.

REFERENCES

[1] Junaid Mohammed, Abhinav Thakral, Adrian Filip Ocneanu, Colin Jones, Chung-Horng Lung, Andy Adler, "Internet of Things: Remote Patient Monitoring Using Web Services and Cloud Computing", *2014 IEEE International Conference on Internet of Things (iThings 2014), Green Computing and Communications (GreenCom2014), and Cyber-Physical-Social Computing (CPSCom 2014), P.P 978-1-4799-5967-9/14.*

[2[Tae-Yoon Kim, Sungkwan Youm, Jai-Jin Jung, Eui-Jik Kim, "Multi-hop WBAN Construction for Healthcare IoT",*2015 International Conference on Platform Technology and Service, P.P 978-1-4799-1888-1/15.*

[3]Boyi Xu, Li Da Xu, Senior Member, IEEE, Hongming Cai, Cheng Xie, Jingyuan Hu, and Fenglin Bu, "Ubiquitous Data Accessing Method in IoT-Based Information System for Emergency Medical Services", IEEE Transactions on Industrial Informatics, Vol. 10, No. 2, May 2014, pp.

[4]H.H.Lee, "Network-based fire-detection system for smart homr automation", *IEEE Transactions on Consumer Electronics,* vol.50, no.4, pp, 1993-1099, 2016.

[5]Zhi-xiaonTu, Cheng-Hong and Hao Feng "EMACS: Design and Implementation of Indoor Environment Monitoring and Control System" Proceedings of the 2017 IEEE ICIS, May 2017.

[6]N.Kiruthikanjali, G.Yuvaraj,"Secured Smart Healthcare Monitoring System based on IoT" Proceedings of the 207 IEEE February 2017.

An Adaptive Routing Protocol for extension of Lifetime and Coverage Area in WSN

Mrs. B. Mary Amala Jenni
Assistant Professor,
Department of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Ms. S. K. Suriya
Assistant Professor,
Department of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Mrs. D. Umamaheswari
Associate Professor,
Department of Electronics and Communication Engineering,
St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti – 607106.

Abstract- The particularities of Wireless Sensor Networks require specially designed protocols. Nodes in these networks often possess limited access to energy (usually supplied by batteries), which imposes energy constraints. Additionally, WSNs are commonly deployed in monitoring applications, which may in- tend to cover large areas. Several techniques have been proposed to improve energy-balance, coverage area or both at the same time. In this paper, an alternative solution is presented. It consists of three main components: Fuzzy C-Means for network clustering, a cluster head rotation mechanism and a sleep scheduling algorithm based on a modified version of Particle Swarm Optimization. Results show that this solution is able to provide an adaptive routing protocol that offers reduced energy consumption, while keeping high- coverage area.

Keywords

Particle Swarm Optimization, Fuzzy C-Means, Clustering, Lifetime

1. Introduction

(WSN) is usually used in the most varied applications such as environmental, industrial and process monitoring. They are formed by distributed sensing devices, commonly powered by batteries that at the end of their lifetime must be either recharged, replaced or even require completely substitution of the device. Any of these cases calls for human interference, which in some scenarios having access to the devices is neither straightforward nor immediate (e.g. remote monitoring of forests). Therefore, while designing WSN architectures and protocols, the presence of low-power techniques are often de-sired. These techniques would allow prolonged network lifetime and possibly extended network coverage. From the architectural point-of-view, techniques such as clustering may help to balance the energy consumption among the network's nodes. Clustering splits the network in subsets called clusters. Cluster members send the sensed information directly to cluster heads, which aggregate the members' messages and forward them to the base station Communicating with the cluster head instead of directly with the base station reduces the energy spent at transmission, because cluster heads are usually near to nodes. Another technique used in conjunction with clustering is to rotate the cluster head role, meaning that all nodes in a cluster can assume that responsi-bility. Thus, instead of overloading a single node with the retransmission/ routing (due to being a cluster head), all nodes share this load at different times, balancing the energy inside the cluster.

-

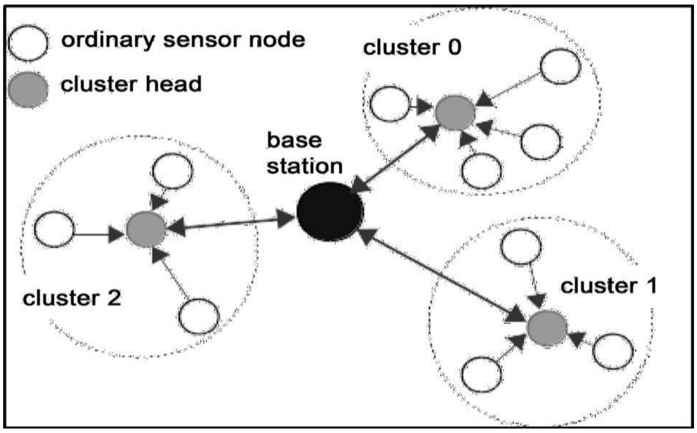


Figure 1. Clusters in WSN.

2. Preliminaries

In this section, the energy model and the coverage/overlapping definitions are briefly explained.

2.1. Energy Model

The energy model adopted in Section 4 is based on [1]. Nodes contains 1 or more sensors, a micro-controller, a transceiver and an energy source.

Regarding the energy model, the sensors are assumed to be passive, *i.e.* they do not consume energy, while the other components are all active. The total energy expenditure depends whether the node is ordinary or if it is a cluster head, since ordinary nodes transmit to the cluster head while cluster heads transmit to the base station. Also, cluster heads need to communicate with every cluster node, while ordinary nodes communicate only with the cluster head.

The transmitter model considers two components: the energy dissipated by the transmitter circuitry, which depends on the length l of the messages being communicated, and the energy dissipated by the power amplifier E_{pa}, which depends on the length of the messages, on the distance to the other communicant and on the channel model. The total energy E_{tx} is represented in Equation (1).

The total energy dissipated in one round (when every node send data to the cluster head and it aggregates and transmits it to the base station) is:

$$\sum{}_{c=1}^{C} \left(E_{da} + E_{rx} + \sum{}_{n=1}^{N_c} E_{tx}\right) \quad (7)$$

where C is the total number of clusters and N_c is the number of nodes in cluster c.

2.2. Coverage and Overlapping Area Definitions

The definitions of coverage and overlapping areas are similar to the ones found in , with minor differences:

- Every node covers a circular area with a predefined radius (dependent on the sensor), *i.e.* the node can monitor that region of space. The union of all node's areas is called network coverage area.
- Areas that are monitored by more than one node (*i.e.* intersection regions) are accounted for overlapping. The union of all these areas is called network over-lapping area.
- Areas that are covered exclusively by one node are called exclusive regions. Areas that are covered by more than one node are called overlapping regions. Coverage rate is the partial network coverage area of a particular configura-tion (when only a subset of nodes are active) over the total network coverage area.

3. Methodology

The proposed solution consists of using FCM for clustering the network, then using a straightforward cluster head rotation mechanism in each round and scheduling sleep slots with the modified PSO, which maximizes both energy-balance and network coverage. The clustering phase and cluster head rotation mechanism is described in Section 4.1 and the modified PSO is described in Sec-tion 4.2.

3.1. Clustering Phase

The first step required in clustering is to determine the optimal number of clus-ters.

E_{fs} is the energy spent in the transmission of a single bit of data through free space, achieving an acceptable bit error rate;

E_{mp} is the energy spent in the transmission of a single bit of data through a *multipath fading* model, achieving an acceptable bit error rate;

d_{toBS} is the average Euclidean distance from the cluster heads to the base sta-tion.

Notice also that E_{fs} and E_{mp} are dependent on the distance of transmission. Once the number of clusters is defined, the FCM algorithm helps to determine both the cluster centroids and the initial assignment of sensor nodes to clusters. For that purpose, the method minimizes the following objective function (Equa-tion (9)):

$$J_m = \sum{}_{i=1}^{C}\sum{}_{j=1}^{N} u_{ij}^{m}\, d_{ij}^{2}, 1 \le m < \infty \quad (2)$$

where u_{ij} is the coefficient representing the degree of membership of the node i w.r.t. the cluster j, d is the Euclidean distance between the i^{th} node and the j^{th} cluster centroid, and m is a real parameter that represents the fuzzyness of the clusters. The u_{ij} coefficients form a coefficient matrix U where i indexes the i^{th} row and j indexes the j^{th} column.

Where d_{kj} is the Euclidean distance between the kth sensor node and the j^{th} clus-ter centroid. Equation (10) shows that the greater the distance between a node and a centroid, the smaller the respective coefficient will be. The matrix U is initialized with random samples from a uniform distribution with values ranging from 0 to 1 (representing a probability).

The cluster centroids are iteratively calculated using Equation (4):

$$c_j = \frac{\sum_{i=1}^{N} u_{ij}^{m} x_i}{\sum_{i=1}^{N} u_{ij}^{m}} \qquad (4)$$

where x_i is the geolocation of the ith node and c_j is the geolocation of the j^{th} clus-ter centroid.

The complete algorithm is show in Algorithm 1. Lines 1 - 3 show the initiali-zation of the matrix U ($U^{(0)}$). Lines 6 - 11 represent an iteration, where for each cluster the centroid is iteratively calculated using Equation (4) (line 9). The membership matrix is updated at each iteration using Equation (3) (line 10). Fi-nally, the FCM algorithm stops either when the error is below some threshold ε, or when the algorithm had run for a certain number of iterations.

After completing, the algorithm has defined the degree of membership of nodes. Then, each node is initially set to belong to the cluster that it has the highest degree of membership.

The base station initially *selects* the node nearest to each cluster centroid as the cluster head. However, the network hierarchy overloads cluster heads: they must relay messages from every cluster node to the base station. Thus, they ex-pend energy faster than ordinary nodes. For this reason, the cluster head selec-tion must be dynamic in order to prevent those nodes to extinguish their energy supplies and to balance the energy load.

Algorithm 1. FCM algorithm for cluster formation.

```
for $i$ = 0 to $N$
for $j$ = 0 to $C$
$u_{ij}^{(0)} \sim uniform(0.0, 1.0)$
$k \leftarrow 0$
repeat
$k \leftarrow k + 1$
for $j$ = 0 to $C$
update cluster centroid $c_j$ using Equation (4)
update $U^{(k)}$ using Equation
(3) 11 until $\|U^{(k)} - U^{(k-1)}\|$
$< \varepsilon$
```

Therefore, after the first round, the current cluster head elects another node to be the new cluster head. It chooses the node with the highest residual energy (this information is sent to the cluster head in every packet). This procedure is repeated every exchange of data, meaning that the cluster head role is reassigned periodically. It is also important to notice that the FCM algorithm is only used at the initial setup of the network. From that moment on, the partitions (clusters) are fixed while the cluster head changes dynamically.

The cluster head is responsible for allocating time slots when cluster members can transmit. This is implemented using a TDMA schedule. Regarding power consumption, cluster members activate their radio component only during their own slots, reducing the power consumption. Also, transmission power is opti-mized since the Euclidean distance between nodes and cluster head is minimized by the FCM algorithm. Additionally, energy is saved due to the fact that data ag-gregation and fusion is executed at the cluster head, which compresses the in-formation sent to the base station.

3.2. Sleep Scheduling

PSO is a computational method that optimizes an objective function by searching the solution space simultaneously with multiple "probes", aiming to improve the proposed solution iteratively. It is inspired by the social behavior of living being herds, where each “probe” is called particle and it represents a can-didate solution. Particles move through the solution space looking for a local op-tima with a certain velocity. At each iteration, each particle velocity is updated proportionally to the particle’s own inertia (algorithm’s parameter) but is also partially redirected to the local (particle’s) best known position and to the global (swarm’s) best known position. Therefore the particle movement (velocity) has three components: an inertial one, a personal one and a social one; simulating the herd’s behavior.

Algorithm 2. Modified PSO Algorithm.

```
for each cluster do
for $i$ = 1 to $P$ do
$p_i \leftarrow initialize\_particle()$
$l_i \leftarrow p_i$
if $i$ = 1 or $fitness(l_i) > fitness(g)$ then
$g \leftarrow l_i$

for it = 1 to M do
for $i$ = 1 to $P$ do
$r_p, r_g \sim uniform(0.0, 1.0)$
$p_i \leftarrow mutation(p_i, \omega)$
if $r_p < \varphi_p$ then
$p_i \leftarrow crossover(p_i, l_i)$
if $r_g < \varphi_g$ then
$p_i \leftarrow crossover(p_i, g)$

if $fitness(p_i) > fitness(l_i)$ then
$l_i \leftarrow p_i$
if $fitness(p_i) > fitness(g)$ then
$g \leftarrow p_i$
```

4. Results and Discussion

The settings common to all scenarios are described below (except when mentioned differently).

The 2-dimensional field where 300 nodes are distributed is 250 × 250 m^2 and the nodes are distributed using an independent uniform distribution for axis x and y. The base station is at (125, 125), *i.e.* the center of the field. The message length is 4000 bits plus a 150 bit header. The coverage radius for every node is 20 meters. The fuzziness factor is equal to 2, and the number of clusters is usually calculated as 5. The initial energy at every node is 2 Joules.

In all simulations, except for the Direct Communication setup, we considered that the base station must regularly broadcast routing/clustering information and sleep scheduling in order to every node know how to proceed in the next round. This forces nodes to spend at least the energy to receive this information (considering a 4150 bit message). Some authors consider that the cluster head perform this functionality while other authors do not consider this step in the energy consumption.

It is also important to note that the results shown in this section do not consider the initial energy spend in case nodes need to send their position to the base station. For the settings described above, this expenditure is equal to 0.303 Joules net or 0.001 Joules per node (in average).

4.1. Scenario: Cluster Formation

In this scenario, we show the cluster formation generated by the FCM algorithm (Figure 3). Nodes are represented as points and each color indicates a different cluster membership. Gray solid lines are the boundaries of each cluster. Red tri-angles represent the cluster centroids while the red cross represent the base station. As mentioned earlier, each node in FCM belong to all clusters with a cer-tain probability. In this plot, we assigned nodes to the most probable cluster.

4.2. Scenario: Network Lifetime

In this scenario, DC, MTE, LEACH, FCM, FCM plus original PSO and FCMMPSO are analyzed from the network lifetime perspective.

As expected using DC makes nodes farther from the base station deplete their batteries first, but nodes nearer to the base station outlive any other algorithm. When using LEACH, nodes tend to survive longer than DC ones. The cluster rotation mechanism used for LEACH randomly selects the next cluster head (as [1]). This mechanism does not take node's remaining energy into account. For this reason it performs poorly.

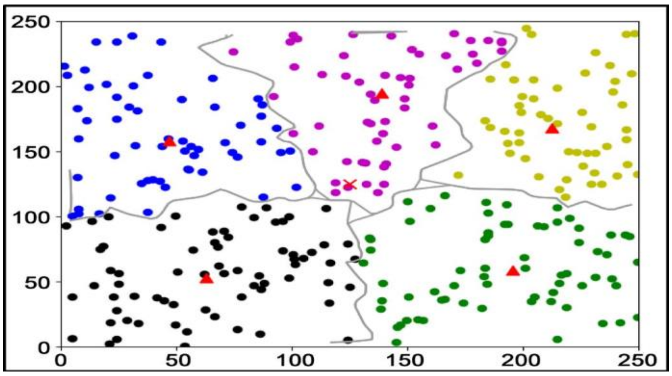


Figure 2. FCM cluster formation.

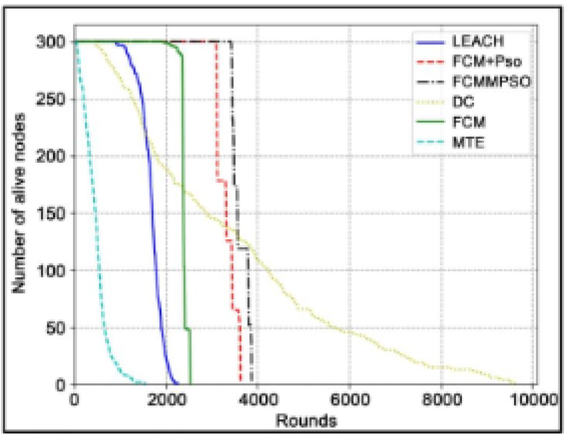


Figure 3. Number of alive nodes vs time (in rounds).

Concerning MTE, nodes nearer to the base station forward messages of all other nodes that are farther from the base station. Therefore, these nodes are overloaded and are depleted quickly. When these nodes are off, the farther nodes have to communicate directly to the base station, and due to the effort of transmitting over larger distances, also get their batteries depleted. As expected, FCM with original PSO perform better than other methods that rely only on clustering. This is straightforward since original PSO decides that some nodes should occasionally sleep, saving their batteries.

As shown, FCMMPSO outperforms all other strategies. It seems that the modified PSO was able to always find solutions that lead to improved network lifetime.

In order to detail the results shown in Figure 3, Table 1 shows the time when the first node depletes its battery and the time when 30% of the nodes die, respectively. Also we included results (for the same distribution/position of nodes) where the base station is decentralized at (125, −75), *i.e.* out of the map.

Figure 4shows the map where the nodes are distributed. Red triangles represent the cluster centroids while the red cross represent the base station. Each area is colored according to the time (round) when the surrounding nodes get their batteries depleted. Dark areas represent nodes that die earlier, while light colors represent nodes that die later in the network lifetime. The base station is at the center of the map *i.e.* at (125, 125).

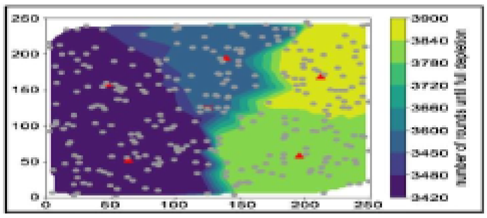


Figure 4. Map with time of depletion for FCMMPSO

Table 1. Round when first node die and when 30% of nodes die (for different algorithms).

Base station at:

Algorithm	(125, 125)		(125, −75)	
	Number of depleted nodes:			
	1	30%	1	30%
DC	430	1685	11	97
MTE	29	312	28	141
LEACH	906	1585	459	1247
FCM	1943	2363	1500	1595
FCM+PSO	3088	3117	1872	1955
FCMMPSO	3422	3477	2033	2102

Since the base station is at the center of the map, those nodes are the last to die (they spend less energy communicating with the base station). As it can be seen, most of the clusters die almost at the same time (have the same color in the map). This means that the network lifetime lasts longer but also that all nodes die approximately together.

4.3. Scenario: Coverage Rate

In this scenario, the effects of the proposed solution on coverage, overlapping and sleeping rates are analyzed. For that purpose, simulations take into account four sets of configurations:

- 0.0 and β = 1.0 (only coverage area is optimized);
- α = 0.25 and β = 0.75 (coverage should be prioritized over lifetime);
- α and β equal to 0.5 (network lifetime and coverage area should be optimized equally);

Table 2. Coverage, overlapping and sleeping rates with different settings for FCMMPSO.

α	β	Coverage rate	Overlapping rate
0.0	1.0	0.95 ± 0.01	0.25 ± 0.04
0.25	0.75	0.90 ± 0.03	0.23 ± 0.05
0.5	0.5	0.88 ± 0.04	0.42 ± 0.08
0.75	0.25	0.83 ± 0.05	0.45 ± 0.09

Table 3. Coverage, overlapping and sleeping rates with different settings for ECCA.

α	β	Coverage rate	Overlapping rate
0.0	1.0	0.89 ± 0.06	0.14 ± 0.07
0.25	0.75	0.87 ± 0.03	0.27 ± 0.07
0.5	0.5	0.86 ± 0.05	0.42 ± 0.08
0.75	0.25	0.84 ± 0.04	0.45 ± 0.08

- α = 0.75 and β = 0.25 (lifetime is more important than coverage).

Results for FCMMPSO are shown in Table 2, while results regarding ECCA [17] are shown in Table 3. Every cell represents the average rate followed by the standard deviation (averaged during the network lifetime).

Results show that FCMMPSO always find better solutions concerning cover-age rate (in comparison to ECCA), reaching a maximum improvement of 6%. It is important to notice that ECCA is based on NSGA-II, which is a multi-objective approach, meaning that by default it does not learn solutions that improve one objective while get worse on the other objective. This imposes a constraint to the learning approach when one wants to prioritize one objective over another. The overlapping rates of both approaches are similar, and both manage to re-duce it to only 25% when b = 1.0 (coverage is the only goal). It is important to notice that for ECCA, the sleeping rate decreases as α increases. This behavior is exactly the opposed to what is expected, since as a increases one would expect to have more sleeping nodes to extend network lifetime, not fewer. This anomaly can be explained due to the fact that NSGA-II does not consider α and β (it is not a multi-objective problem converted to single-objective by using a weighted sum).

4.4. Scenario: Energy

In order to analyze the energy savings, five simulations were considered, with increasing levels of the hyperparameter α (and therefore decreasing levels of the hyperparameter β). Figure 6 shows the relation between coverage rate and number of active nodes. In this scenario, 100 nodes are used. For the higher coverage rate (0.9 to 1), FCMMPSO is more effective in covering more area with less active nodes than ECCA. It must be noticed that even if this result depends on the distribu-tion of the nodes in the map, all simulations showed that FCMMPSO always uses less nodes for the same coverage rate.

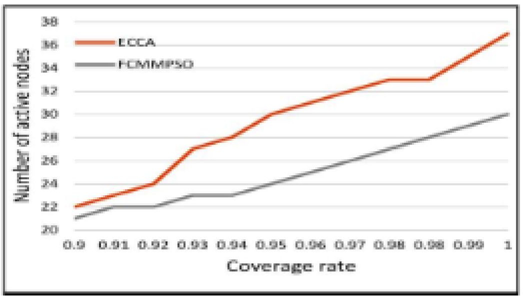


Figure 5. Coverage rate vs number of active nodes.

5. Conclusion

We presented an alternative solution to improve network lifetime while maximizing network coverage area. FCM is used for network clustering, by splitting the network in small subsets where transmission power is kept low. Additionally, each cluster has a head rotation mechanism that seeks to prevent low-energy nodes from communicating directly to the base station, resulting at a better energy-balance. On top of that, sleep slots are distributed among cluster nodes, in order to extend network lifetime. Better configurations of sleep schedules are found using the modified PSO algorithm that searches for both saving-energy and high-coverage rate configurations. Results show that, by correctly setting up PSO hyper parameters, the algorithm is able to learn better configurations and thus provide meet the specifications of applications with different goals.

References

[1] Dhawan, H. and Waraich, S. (2014) A Comparative Study on LEACH Routing Pro-tocol and Its Variants in s: A Survey. *International Journal of Computer Applications*, 95, 21-27. https://doi.org/10.5120/16614-6454

[2] Hoang, D.C., Kumar, R. and Panda, S.K. (2010) Fuzzy C-Means Clustering Protocol for s. *IEEE International Symposium on Industrial Elec-tronics*, Bari, 3477-3482. https://doi.org/10.1109/ISIE.2010.5637779

[3] Deng, J., Han, Y.S., Heinzelman, W.B. and Varshney, P.K. (2005) Balanced-Energy Sleep Scheduling Scheme for High Density Cluster-Based Sensor Networks. *Elsevier Computer Communications Journal*, 28, 1631-1642.

[4] Sekhar, S. (2005) A Distance Based Sleep Schedule Algorithm for Enhanced Life-time of Heterogeneous s. Master’s Thesis, University of Cincinnati.

[5] Pearlman, M.R., Deng, J., Liang, B. and Haas, Z.J. (2002) Elective Participation in Ad Hoc Networks Based on Energy Consumption. *Proceedings of IEEE Global Tel-ecommunications Conference*, November 2002, 26-31. https://doi.org/10.1109/GLOCOM.2002.1188035

[6] Yu, C., Guo, W. and Chen, G. (2012) Energy-Balanced Sleep Scheduling Based on Particle Swarm Optimization in. 26*th International Paral-lel and Distributed Processing Symposium Workshops & PhD Forum*, Shanghai, 1249-1255. https://doi.org/10.1109/IPDPSW.2012.154

[7] Kennedy, J. and Eberhart, R. (1995) Particle Swarm Optimization. *Proceedings of IEEE International Conference on Neural Networks*, Vol. 4, 1942-1948. https://doi.org/10.1109/ICNN.1995.488968

[8] Chelbi, S., Dhahri, H., Abdouli, M., Duvallet, C. and Bouaziz, R. (2016) A New Hy-brid Routing Protocol for s. *International Journal of Ad Hoc and Ubituitous Computing*.

TABLE OF CONTENT

COMPUTER SCIENCE AND ENGINEERING

Multi Auditable Outsourced Eliptical Curve Cryptography Based Access Control in Cloud Computing

Ms. R.Anupriya, Ms. B.Priyanka, Ms. S.Swathi
UG Students
MRK Institute of Technology, Kattumannarkoil

Mr. R.Gunasekaran
Assistant Professor,
Department of Computer Science and Engineering
MRK Institute of Technology, Kattumannarkoil.

Abstract*—Access control methods ensure that authorized user access data of the system. Access control is a policy or procedure that allows, denies or limits access to system. It also monitors and record all attempts made to access a system. Access Control can also identify unauthorized users attempting to access a system. It is a mechanism which is very much imperative for protection in computer security. A big challenge to data access control scheme is data hosting and data access services. Because data owners do not totally trust the cloud servers also they can no longer rely on servers to do access control, so the data access control becomes a challenging issue in cloud storage systems. So in this paper, can implement trust based authentication system using central authority in cloud system. In existing difficult to predict the attribute authority who is nearest to cloud users. In this paper, also implement geo-location based multi attribute authority authentication system to choose authority nearest to their locations and get the attribute keys from central for trusted framework. And also implement verifiable outsourced decryption to secure the data from unauthorized users with fingerprint schemes. Experimental results show that implement in real time cloud storage system to provide improved access control system.

***Index Terms* - Access control, Geo-location, Cloud storage system, Attribute authorities, Trusted framework**

I. INTRODUCTION

Access control is generally a policy or procedure that allows, denies or restricts access to a system. It may, as well, monitor and record all attempts made to access a system. Access Control may also identify users attempting to access a system unauthorized. It is a mechanism which is very much important for protection in computer security. Various access control models are in use, including the most common Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC). All these models are known as identity based access control models. In all these access control models, user (subjects) and resources (objects) are identified by unique names. Identification may be done directly or through roles assigned to the subjects. These access control methods are effective in unchangeable distributed system, where there are only a set of Users with a known set of services. Nowadays, very large distributed open systems are developing very rapidly. These include Grid Computing and Cloud Computing. These systems are like virtual organizations with various autonomous domains. The relationship between users and resources is dynamic and more ad-hoc in cloud and inter cloud systems. With the development of large distributed systems attribute based access control (ABAC) has become increasingly important. The basic cloud is shown in fig 1.

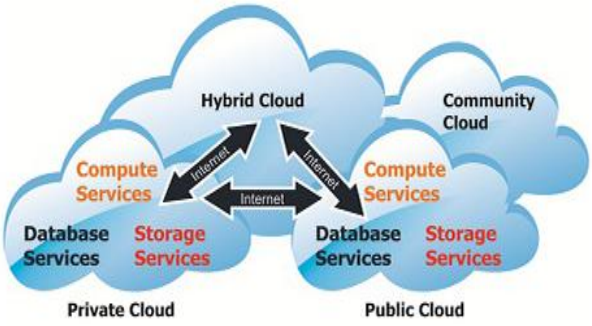


Fig 1.1 - Cloud deployment model

II. RELATED WORK

Ning,Jianting, et al. investigated the interesting problems and further propose a new notion called auditable σ -time outsourced CP-ABE. Specifically, present a basic outsourced CP-ABE system in the key encapsulation mechanism (KEM) setting based on Rouselakis and Waters CP-ABE as the first step. To the best of knowledge, this is the first of its type that supports properties such as secure decryption outsourcing, auditability of decryption, limited and anonymous fine-grained access control, key-leakage resistance and light decryption cost on user side. In addition, the access control mechanism is "anonymous" and "access unlinkable" in the sense that the cloud cannot identify who is "under" the current access and meanwhile, the current access cannot be linked back to the previous ones (assuming the label of current access. Providing the outsourced decryption service for data user, it returns "partial decrypted" cipher text, i.e. transformed cipher text. Note that hereafter will use the term "transformed cipher text".

Joseph A Akinyele, et.al, … [2] proposed a new, extensible and unified framework for rapidly prototyping experimental cryptographic schemes and leveraging them in system applications. Charm is built around the concepts of extensibility, composability, and modularity. The framework is implemented in Python, a well-supported high-level language, designed to reduce development time and code complexity while promoting component re-use.

Matthew Green, et.al,… [3] analyzed new methods for efficiently and securely outsourcing decryption of ABE cipher texts. The core change to outsource able ABE systems is a modified Key Generation algorithm that produces two keys. The first key is a short El Gamaltype secret key that must be kept private by the user. The second is what call a "transformation key", TK, that is shared with a proxy (and can be publicly distributed).If the proxy then receives a ciphertext CT for a function f for which the user's credentials satisfy, it is then able to use the key TK to transform CT into a simple and short El Gamal ciphertext of the same message encrypted under the user's key SK.

Junzuo Lai, et.al,… [4]focused on CP-ABE with verifiable outsourced decryption. The same approach applies to KP-ABE with verifiable outsourced decryption, which will omit here in order to keep the paper compact. To assess the performance of ABE scheme with verifiable outsourced decryption, implement the CP-ABE scheme with verifiable outsourced decryption and conduct experiments on both an ARM-based mobile device and an Intel-core personal computer to model a mobile user and a proxy, respectively. The software is based on the CP-ABE implementation in the libfenc library.

Jin Li,et.al,…[5] propose a generic construction of attribute-based access control system under an interesting architecture, in which two cloud service providers (CSPs) namely key generation-cloud service provider (KG-CSP) and decryption-cloud service provider (D-CSP) are involved to perform the outsourced heavy tasks for users' key issuing and file access. With the help of the CSPs, the computational complexity at both user and attribute authority sides is reduced.

III. IDENTITY BASED ENCRYPTION SCHEMES

Cloud Storage indicates "the limit of records online inside the cloud," wherein the facts are secured in and to be had from the distinct spread and related property that deal a cloud. In any case, the conveyed stockpiling isn't always in reality trusted. Whether the records installation left on the cloud is or now not modifications right into a giant pressure of the clients. So to comfy records and client Identity; Identity Based Encryption (IBE) is a captivating choice that is planned to streamline key combination in an approval, in moderate of Public Key Infrastructure (PKI) through via human realistic Identities (e.g., uncommon call, electronic mail deal with, IP deal with, and whatnot) as open keys. An IBE method which normally includes entities, PKG, and clients (together with sender and receiver) has consisted of the subsequent 4 algorithms.

Setup(λ) : The system set of rules takes as input a protection parameter λ and outputs the majority key PK and the grasp key MK. Note that the grasp secret's saved mystery at PKG.

KeyGen(MK,ID) : The private key era set of rules is run via PKG, which takes as enter the master key MK and person's identity ID $\in$ 0, 1. It returns a private key SKID parallel to the identity ID.

Encrypt (M, ID): The encryption set of rules is administered by the use of sender, which takes as enter the receiver's identity ID and a spatial statistics M to be encrypted. It outputs the cipher text CT.

Decrypt (CT, SKID): The decryption set of policies is run through receiver, which takes as input the cipher text CT and his/her personal key SKID. It proceeds a spatial statistics M or an errors $\perp$.

An IBE method has to assure the description of reliability. Particularly, whilst the personal key SKID generated through set of rules KeyGen whilst it is given ID because the input, then Decrypt (CT, SKID) = M in which CT = Encrypt (M, ID). The inspiration of IBE is to simplify certificates manage. The workflow shape of IBE is demonstrated in fig 2.

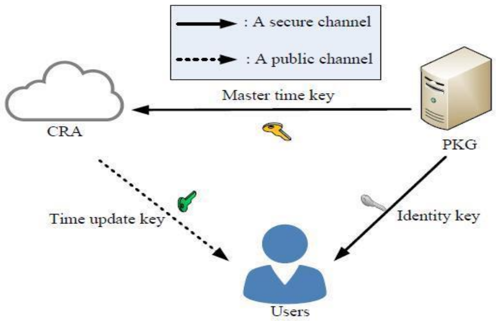


Figure 3.1. - Work Flow of IBE

3.1 Identity based encryption without random oracles:

Since the arbitrary prophet version be pretty contentious, a crucial open hassle after the development of changed into to build up a person based encryption plot it's probably cozy in the stylish model. As a preliminary move inside the path of this aim, Canetti et al. [8] make a persona primarily based encryption conspire that is probably cozy without arbitrary prophets, no matter the fact that in a fairly weaker safety display. In this debilitated model, known as a unique man or woman safety, an enemy wants to cognizance on the individual he desires to bother in progress of time. In the normal individual primarily based totally version, the enemy is permitted to adaptively pick out his purpose man or woman. The protection of the plan relies on upon the stability of the DBDH trouble and the improvement is very wasteful.

3.2 Hierarchical identity based encryption:

The idea of numerous leveled individual based completely encryption turned into first of all provided by means of Horwitz and Lynn [12]. In usual open key infrastructures, there can be a source testament expert, and conceivably a development of different authentication experts. The source professional can trouble authentications to specialists on a lower stage and the decrease diploma endorsement specialists can hassle testaments to customers. To lower workload, a comparable setup might be precious inside the setting of man or woman based encryption. In character primarily based encryption the trusted celebration is the personal key producer.

3.3 Fuzzy identity based encryption

In [15], Sahai and Waters provide a Fuzzy identification based absolutely encryption framework. In Fuzzy identification based encryption, characters are visible as an arrangement of clean functions, as opposed to a sequence of characters. The concept is that non-public keys can unscramble messages encoded with the overall populace key ϕ, additionally, messages scrambled with humans in famous key ϕ' if $d(\phi, \phi') < e$ for a particular metric d and a version to non-crucial failure esteem e. One significant use of fluffy man or woman primarily based completely encryption is the usage of biometric personalities.

3.4 Identity based encryption schemes without pairings

Another individuality primarily based encryption conspires so as to grow to be distributed spherical an indistinguishable time from the Boneh-Franklin plot (yet ended up being designed quite a long whilst previous) is because of Cocks. The protection of the framework depends at the quadratic residuosity trouble modulo a composite N = p, q where p, q ε Z are top [19]. Lamentably, this framework gives you big determine writings contrasted with the mixing based totally frameworks and along those lines isn't always especially effective.

IV. ATTRIBUTE BASED ENCRYPTION

An Attribute based encryption scheme brought by means of way of Sahai and Waters in 2005 and the cause is to provide protection and get proper of entry to manipulate. Attribute-based encryption (ABE) is a public-key based actually one too many encryptions that allow users to encrypt and decrypt data based on personal attributes. In which the name of the game key of a consumer and the cipher textual content is primarily based upon attributes. In the form of tool, the decryption of a cipher textual content is feasible first-class if the set of attributes of the individual key suits the attributes of the cipher textual content. Decryption is fine feasible whilst the amount of matching is at least a threshold price d. Collusion-resistance is a crucial protection characteristic of Attribute-Based Encryption. The application of this scheme is restricted inside the actual environment because it uses the get entry to of monotonic attributes to govern patrons get admission to inside the device.

4.1. Key Policy Attribute Based Encryption (KP-ABE):

It is the modified form of the traditional version of ABE. Users are assigned with a get right of access to tree shape over the information attributes. Doorstep gates are the nodes of the get right of entry to the tree. The attributes are connected thru leaf nodes. To replicate the get right of entry to tree configuration the decision of the game key of the man or woman is defined. Cipher texts are categorized with gadgets of attributes and personal keys are connected with monotonic way in systems that manage which cipher texts a client is capable to decrypt. Key Policy characteristic Based Encryption (KP-ABE) method is considered for one-to-many communications.

4.2. Cipher Text Policy Attribute Based Encryption:

One more changed shape of ABE known as CP-ABE introduced through Sahai. In a CP-ABE scheme, each cipher textual content is connected with a get right of entry to insurance on attributes, and everyone's non-public key is related to a hard and fast of attributes. A purchaser is capable of decrypting a cipher textual content only if the set of attributes associated to the customer's personal key satisfies the get right of entry to insurance related to the cipher text. CP-ABE works the other manner of KP-ABE. The most cutting-edge-day ABE schemes are derivative from the CPABE method.

4.3. Attribute-based Encryption Scheme with Non- Monotonic Access Structures

Preceding ABE schemes had been reserved to expressing satisfactory monotonic get right of entry to structures and there may be no remarkable technique to correspond to horrible constraints in a keys receives right of access to additives. Non-monotonic right of entry shape can use the awful word to explain each attribute in the message, but the monotonic get admission to the structure can't.

4.4. Hierarchical attribute-based Encryption

This device is known as Hierarchical characteristic-primarily based encryption (HABE) that is derived with the resource of cloud structure. The HABE prototypical incorporates with root manager (RM) that resembles to provide the value 0.33 depended on Trusted third party (TTP), a couple of data masters (DMs) wherein the pinnacle-level DMs parallel to more than one organization customers, and several customers that parallel to altogether employees in a group. This shape recycled the possessions of classified generation of explanations in HIBE scheme in the direction of keys to supply. The hierarchical shape is proven in fig 3.

Then, HABE shape is nicely-defined by means of the usage of offering randomized polynomial period algorithms as follows:

Setup (K) implies (params, MK0): The RM proceeds a correctly massive protection parameter K as entering, and yields storage parameters as params and root master key MK0 for initial system.

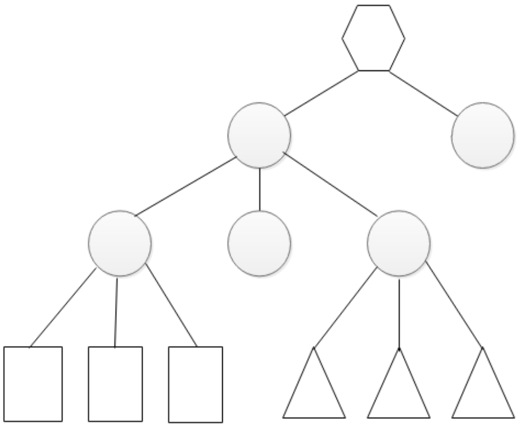


Figure 4.1- Hierarchical data structure

CreateDM(params, MKi, PKi+1) implies (MKi+1): Whether the RM or the DM generates grasp keys for the DMs immediately underneath that one the usage of params and its primary key in system.

Create User (params, PKu, PKa, MKi) implies (SKi, U, SKi, U, a): The DM ends in tests whether or not or not U is eligible for a this is controlled with the useful resource of themselves. If so, it produces a person identification stealthy key and a personal representative stealthy key for U, the use of params and its primary key; in any other case, it outputs returned as NULL values

Encrypt(params; f; X; x E X)→(CT): A man or woman takes a document f, a DNF get right of entry to manipulate coverage X, and commonplace keys of all traits in X, as entering, and results in a ciphertext CT in storage

Decrypt(params, SKi,u, CT, x, ECCj→(f) implies A character, whose tendencies gratify the jth conjunctive part CCj, proceeds params, the person identity secret key, the ciphertext, and the individual function secret keys on complete attributes in CCj, as inputs, towards to get higher the unique textual content. In that machine can gratify the assets of satisfactory grained get entry to regulate the scalability and whole delegation. And can segment the records for consumers in the cloud in organization surroundings.

4.5. Multi-Authority Attribute Based Encryption (MA-ABE):

This structure uses numerous activities to allocate tendencies aimed at various clients. MA-ABE tool consists of number of K function of authority and precise vital professional. Every characteristic authority remains likewise allocated with nicely worth dk. The device makes use of the succeeding algorithms:

Setup: This algorithm with randomized attributes that has to remain analyzed through using way of the use of some depended on parties (for example Central authority). The input can assign as privacy parameter, Yields a public key, actioner key pair for every of the characteristic authority, and furthermore outputs a tool public key and maintain close actioner key in a manner to be utilized by the important consultant.

Attribute Key Generation: Key generation can be provided a set of pointers run through a featured authority. Takings as input with authorities master key and with the authority's value dk, someone's group ID, and a set of characteristics in the authority's vicinity (It will count on that the consumers declare of those features have remained tested earlier than with the set of regulations is administered). Outcome is master key for the customer.

Central Key Generation: List out the set policies in randomized format runs through the way of the manner of the crucial expert. Takes as the message as input that hold the close master key and a person's GID and outputs actioner key for the consumer.

Encryption: It algorithms and takes input text as randomized format runs through a sender. Takes as input a tough and fast of attributes for each specialist, a message, and the gadget public key which is common to all.Outputs the cipher textual content.

Decryption: It is a deterministic set of rules runs with the aid of someone. Takes as contribution a cryptogram text, it became encrypted beneath feature set AC and decoded keys for a characteristic >dk for all experts that are enough in cloud system The proposed tool version consists of five entities: named as Central authority denoted as CA, Multiple Attribute Authority denoted as AAs, Data owner (Owners), Clients (Users), and a cloud service provider with various cloud servers. The proposed structure of MA-ABE is shown in fig 6.

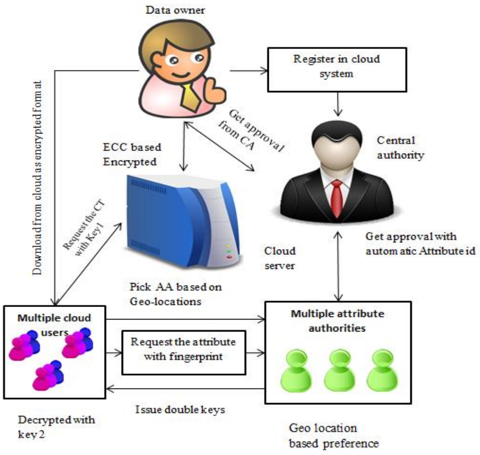

Data owner
Register in cloud system
Central authority
Get approval from CA
ECC based Encrypted
Download from cloud as encrypted format
Request the CT with Key1
Cloud server
Get approval with automatic Attribute id
Pick AA based on Geo-locations
Multiple cloud users
Request the attribute with fingerprint
Multiple attribute authorities
Issue double keys
Decrypted with key2
Geo location based preference

Figure 4.2 - Proposed Framework

V. EXPERIMENTAL RESULTS

From the above definition considered one of a kind encryption patterns reading with the unique strategies and constraints. KP-ABE strategies with encryption provide low and excessive associated with encryption process with the get admission to manipulate constraints. This paper employed the above algorithms at one degree must be more than a preceding stage, for this the revisions the overall performance of diverse algorithms enslavement on the general overall performance of set of regulations used at one stage is used to decide the following stage. In this way the set of rules implemented at numerous degree of classified result is modified to predict most degree of overall performance. And proposed multi authority feature based totally encryption also assist get proper of entry to suggestions based totally on purchaser call for or function revocation below emergency eventualities. The typical overall performance consequences shown in fig 7 based on response time for retrieving spatial records from cloud garage.

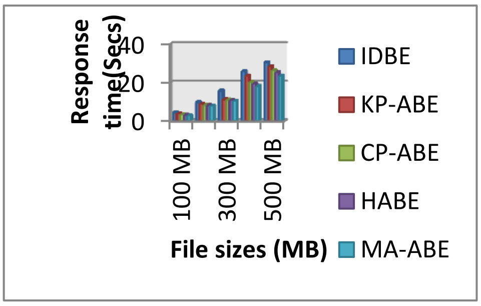


Figure 5.1- Performance chart

VI. CONCLUSION

In this paper, we proposed a new framework to eliminate the single-point performance bottleneck of the existing CP-ABE schemes. By effectively reformulating CPABE cryptographic technique into our novel framework, our proposed scheme provides a fine-grained, robust and efficient access control with one-*CA*/multi-*AA*s for public cloud storage. Our scheme employs multiple *AA*s to share the load of the time-consuming legitimacy verification and standby for serving new arrivals of users' requests. We also proposed an auditing method to trace an attribute authority's potential misbehavior. The key objective of our framework is to provide security cloud data using Multi Attribute Authority-ECC Based Encryption using multi central authority, that can support efficient attribute, file. These systems also provide backward and forward security.

REFERENCES

1. Joseph A Akinyele, Christina Garman, Ian Miers, Matthew W Pagano, Michael Rushanan, Matthew Green, and Aviel D Rubin. Charm: a framework for rapidly prototyping cryptosystems. Journal of Cryptographic Engineering, 3(2):111–128, 2013.
2. Matthew Green, Susan Hohenberger, and Brent Waters.Outsourcing the decryption of abeciphertexts.In USENIX Security Symposium, volume 2011, 2011.
3. Junzuo Lai, Robert H Deng, Chaowen Guan, and JianWeng. “Attribute based encryption with verifiable outsourced decryption” IEEE Transactions on Information Forensics and Security, 8(8):1343–1354, 2013.
4. Jin Li, Xiaofeng Chen, Jingwei Li, ChunfuJia, Jianfeng Ma, and Wenjing Lou. “Fine-grained access control system based on outsourced attribute-based encryption”. In Computer Security–ESORICS 2013, pages 592–609. Springer, 2013.
5. B. Zhang, J. Wang, K. Ren, and C. Wang, “Privacy assured Trans. Emerging Topics Comput., vol. 1, no. 1, p. 166–177, Jul. Dec. 2013 outsourcing of image reconstruction service in cloud,” IEEE.
6. B. Zhang, J. Wang, K. Ren, and C. Wang, “Privacyassured outsourcing of image reconstruction service in cloud,” IEEE Trans. Emerging Topics Comput., vol. 1, no. 1, p. 166–177, Jul./Dec. 2013.
7. R. Canetti, S. Halevi, and J. Katz, “A forward-secure public-key encryption scheme,” in Advances in Cryptology (EUROCRYPT“03),E. Biham, Ed. Berlin, Germany: Springer, 2003, vol. 2656, pp. 646–646
8. D. Boneh and X. Boyen, “Efficient selective-id secure identity-based encryption without random oracles,” in Advances in Cryptology (EUROCRYPT“04), C. Cachin and J. Camenisch, Eds. Berlin,Germany: Springer, 2004, vol. 3027, pp. 223–238.
9. D. Boneh and X. Boyen, “Secure identity based encryption without random oracles,” in Advances in Cryptology (CRYPTO“04),M. Franklin, Ed. Berlin, Germany: Springer, 2004, vol. 3152, pp. 197– 206.
10. B. Waters, “Efficient identity-based encryption without random oracles,” in Advances in Cryptology (EUROCRYPT“05), R. Cramer, Ed. Berlin, Germany: Springer, 2005, vol. 3494, pp. 114–127
11. C. Gentry, “Practical identity-based encryption without random oracles,” in Advances in Cryptology (EUROCRYPT“06), S. Vaudenay, Ed. Berlin, Germany: Springer, 2006, vol. 4004, pp. 445–464.
12. C. Gentry, C. Peikert, and V. Vaikuntanathan, “Trapdoors for hard lattices and new cryptographic constructions,” in Proc. 40th Annu. ACM Symp.Theory Comput. (STOC“08), 2008, pp. 197–206.
13. S. Agrawal, D. Boneh, and X. Boyen, “Efficient lattice (h)ibe in the standard model,” in Advances in Cryptology (EUROCRYPT“10), H. Gilbert, Ed. Berlin, Germany: Springer, 2010, vol. 6110, pp. 553–572.
14. Y. Hanaoka, G. Hanaoka, J. Shikata, and H. Imai, “Identity-based hierarchical strongly key-insulated encryption and its application,” in Advances in Cryptology

(ASIACRYPT‟05), B. Roy, Ed. Berlin, Germany: Springer, 2005, vol. 3788, pp. 495–514.

15. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology (CRYPTO), G. Blakley and D. Chaum, Eds. Berlin, Germany: Springer, 1985, vol. 196, pp. 47–53.
16. Cocks, "An identity based encryption scheme based on quadratic residues," in Cryptography and Coding, B. Honary, Ed. Berlin/ Heidelberg: Springer, 2001, vol. 2260, pp. 360–363.
17. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," in Advances in Cryptology (EUROCRYPT‟10), H. Gilbert, Ed. Berlin, Germany: Springer, 2010,vol. 6110, pp. 523–552
18. Boneh, X. Ding, G. Tsudik, and C. Wong, "A method for fast revocation of public key certificates and security capabilities," in Proc. 10th USENIX Security Symp., 2001, pp. 297–308.
19. B. Libert and J.-J.Quisquater, "Efficient revocation and threshold pairing based cryptosystems," in Proc. 22nd Annu. Symp.Principles Distrib.Comput., 2003, pp. 163–171.

Efficient Fine Grained Access Control with Semantic Keyword Search on Encrypted Cloud Storage

Ms. G. Aanchana, Ms. V.Harshaeni, Ms. G.Sivaranjani
UG Students
Department of Computer Science and Engineering
MRK Institute of Technology, Kattumannarkoil

Mr. S.Ramalingam
Assistant Professor,
Department of Computer Science and Engineering
MRK Institute of Technology, Kattumannarkoil

Abstract*— Data intensive world, cloud computing is new type of computing paradigm which enables sharing of computing resources over the internet. The cloud characteristics are on-demand self-service, location independent network access, ubiquitous network access and usage based pay. Due to this charming features private and public organization are outsourcing their large amount of data on cloud storage. Organizations are motivated to migrate their data from local site to central commercial public cloud server. By outsourcing data on cloud users gets relief from storage maintenance. Although there are many benefits to migrate data on cloud storage it brings many security problems. Therefore the data owners hesitate to migrate the sensitive data. In this case the control of data is going towards cloud service provider. This security problem induces data owners to encrypt data at client side and outsource the data. By encrypting data improves the data security but the data efficiency is decreased because searching on encrypted data is difficult. The search techniques which are used on plain text cannot be used over encrypted data. The existing solutions supports only identical keyword search, semantic search is not supported. In the project we proposed semantic multi-keyword ranked search system with verifiable outsourced decryption in multi cloud framework. The data owner uploads files and then encrypt using ECC algorithm and split into multiple formats. To improve search efficiency this system includes semantic search by using fuzzy search.

Index Terms—**Semantic keyword search, Data security, ECC encryption, Fuzzy Search, Data outsourcing**

I. INTRODUCTION

Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services), which can be rapidly provisioned and released with minimal management effort. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in either privately owned, or third-party data centers that may be located far from the user–ranging in distance from across a city to across the world. Cloud computing relies on sharing of resources to achieve coherence and economy of scale, similar to a utility (like the electricity grid) over an electricity network. Advocates claim that cloud computing allows companies to avoid up-front infrastructure costs (e.g., purchasing servers). As well, it enables organizations to focus on their core businesses instead of spending time and money on computer infrastructure. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables Information technology (IT) teams to more rapidly adjust resources to meet fluctuating and unpredictable business demand. Cloud providers typically use a "pay as you go" model. This will lead to unexpectedly high charges if administrators do not adapt to the cloud pricing model. While the storage of corporate data on remote servers is not a new development, current expansion of cloud computing justifies a more careful look at its actual consequences involving privacy and confidentiality issues. As users no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted. In particular, simply downloading all the data for its integrity verification is not a practical solution due to the expensiveness in I/O and transmission cost across the network. Besides, it is often insufficient to detect the data corruption only when accessing the data, as it does not give users correctness assurance for those un-accessed data and might be too late to recover the data loss or damage. To fully ensure the data integrity and save the cloud users' computation resources as well as online burden, it is of critical importance to enable public auditing service for cloud data storage, so that users may resort to an independent cloud server to audit the outsourced data when needed. The basic cloud framework is shown in fig 1.

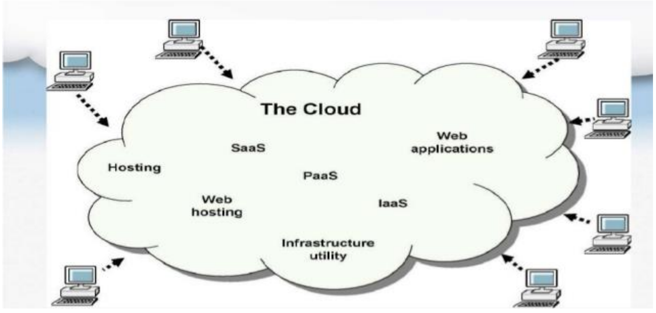


Fig 1.1 - Cloud Computing Framework

II. RELATED WORK

J. Tang, et.al,…[1] proposed The novel cryptographic primitives and various security protection proposals for cloud data services have been presented recently. They can be broadly classified into four categories: confidentiality-assured cloud data service, owner-controlled cloud data sharing, integrity guaranteed cloud data storage, and privacy-preserving cloud data access. More specifically, searchable encryption and homomorphic encryption techniques are proposed to enforce secure data search and data computation, respectively; selective encryption and attribute-based encryption techniques are introduced to achieve authorized access and secure data sharing; provable data possession and proof-of-retrievability techniques are presented to ensure data intactness and retrievability; and privacy preservation is enabled to protect multiple dimensions of private information (e.g., access pattern, query privacy, and identity information) when users access the data stored in the cloud

R. Curtmola, et.al,…[2] implemented private-key storage outsourcing allows clients with either limited resources or limited expertise to store and distribute large amounts of symmetrically encrypted data at low cost. Since regular private-key encryption prevents one from searching over encrypted data, clients also lose the ability to selectively retrieve segments of their data. To address this, several techniques have been proposed for provisioning symmetric encryption with search capabilities; the resulting construct is typically called searchable encryption. The area of searchable encryption has been identified by DARPA as one of the technical advances that can be used to balance the need for both privacy and national security in information aggregation systems.

W. Sun et.al,.. [3] analyzedthe primary hurdles that prevent the widespread adoption of the cloud by potential users, especially if their sensitive data are to be outsourced to and computed in the cloud. Examples may include financial and medical records, and social network profiles. Cloud service providers (CSPs) usually enforce users' data security through mechanisms like firewalls and virtualization. However, these mechanisms do not protect users' privacy from the CSP itself since the CSP possesses full control of the system hardware and lower levels of software stack. There may exist disgruntled, profiteered, or curious employees that can access users' sensitive information for unauthorized purposes. Although encryption before data outsourcing can preserve data privacy against the CSP, it also makes the effective data utilization, such as search over encrypted data, a very challenging task. Without being able to extract useful information from the outsourced data in a secure and private manner, the cloud will merely be a remote storage which provides limited value to all parties.

N. Cao, et.al,…[4] defined and solve the problem of multi-keyword ranked search over encrypted cloud data (MRSE) while preserving strict system-wise privacy in the cloud computing paradigm. Among various multi-keyword semantics, we choose the efficient similarity measure of "coordinate matching", i.e., as many matches as possible, to capture the relevance of data documents to the search query. Specifically, we use "inner product similarity", i.e., the number of query keywords appearing in a document, to quantitatively evaluate such similarity measure of that document to the search query. During the index construction, each document is associated with a binary vector as a sub-index where each bit represents whether corresponding keyword is contained in the document.

Z. Xia, et.al,…[5] proposed a secure tree-based search scheme over the encrypted cloud data, which supports multi-keyword ranked search and dynamic operation on the document collection. Specifically, the vector space model and the widely-used "term frequency (TF) × inverse document frequency (IDF)" model are combined in the index construction and query generation to provide multi-keyword ranked search. In order to obtain high search efficiency, we construct a tree-based index structure and propose a "Greedy Depth-first Search" algorithm based on this index tree. Due to the special structure of our tree-based index, the proposed search scheme can flexibly achieve sub-linear search time and deal with the deletion and insertion of documents. The secure kNN algorithm is utilized to encrypt the index and query vectors, and meanwhile ensure accurate relevance score calculation between encrypted index and query vectors.

III. EXISTING SYSTEM

Cloud outsource storage is one of important services in cloud computing. Cloud users upload data to cloud servers to reduce the cost of managing data and maintaining hardware and software. To ensure data confidentiality, users can encrypt their files before uploading them to a cloud system. However, retrieving the target file from the encrypted files exactly is difficult for cloud server. While Searchable Encryption (SE) has been widely studied, adapting it to the multi-user setting whereby many users can upload secret files or documents and delegate search operations to multiple other users still remains an interesting problem. In this paper we show that the adversarial models used in existing multi-user searchable encryption solutions are not realistic as they implicitly require that the cloud service provider cannot collude with some users. We then propose a stronger adversarial model, and propose a construction which is both practical and provably secure in this new model. The new solution combines the use of bilinear pairings with private information retrieval and introduces a new, non-trusted entity called "proxy" to transform each user's search query into one instance per targeted file or document.

3.1. Boolean Keyword Search Over Encrypted Data

Existing system focused on Boolean Keyword Searchable Encryption. This technique has two drawbacks. In this scheme user have to processes each and every returned file to find the desired one, because user aware of a pre-knowledge of the encrypted cloud data.

3.2. Secure KNN Algorithm:

This system focuses on query processing over encrypted cloud database. In this scheme the distance between the documents and query are computed to find the nearest neighbor to the query. In secure KNN technique first data owner encrypt each attribute of database is encrypted. And the encrypted database is stored on cloud. The authorized user who want access k closest documents to his query, encrypt the query keywords and the encrypted tokens are send to cloud server for searching. The database as well as query is encrypted therefore the query and database confidentiality is preserved.

IV. PROPOSED SYSTEM

In cloud computing, scalable and elastic storage and computation resources are provisioned as measured services through the Internet. Outsourcing data services to the cloud allows organizations to enjoy not only monetary savings, but also simplified local IT management since cloud infrastructures are physically hosted and maintained by the cloud providers. To minimize the risk of data leakage to the cloud service providers, data owners opt to encrypt their sensitive data, e.g., health records, financial transactions, before outsourcing to the cloud, while retaining the decryption keys to themselves and other authorized users. This in turn renders data utilization a challenging problem.

For example, in order to search some relevant documents amongst an encrypted data set stored in the cloud, one may have to download and decrypt the entire data set. This is apparently impractical when the data volume is large. Thus, mechanisms that allow users to search directly on the encrypted data are of great interest in the cloud computing era., efficient multi-keyword fuzzy search over encrypted data remains a challenging problem. We want to point out that the efforts on search over encrypted data involve not only information retrieval techniques such as advanced data structures used to represent the searchable index, and efficient search algorithms that run over the corresponding data structure, but also the proper design of cryptographic protocols to ensure the security and privacy of the overall system. Although multi-keyword search and fuzzy search have been implemented separately, a combination of the two does not lead to a secure and efficient multi-keyword fuzzy search scheme.

In this paper, we propose a brand new idea for achieving multi-keyword (conjunctive keywords) fuzzy search. Different from existing multi-keyword search schemes, our scheme eliminates the requirement of a predefined keyword dictionary. The fuzziness of the keyword is captured by an innovative data structure and algorithmic design without expanding the keyword index, and hence exhibits a high efficiency in terms of computation and storage. Besides the search result, the cloud server should not deduce any keyword information of the file set from secure indexes and trapdoors. Keyword privacy requires indexes and queries be properly represented and securely encrypted. The need of a pre-defined dictionary is a limiting factor that makes dynamic data operations, such as dataset/index update, very difficult. In our design, we would like to eliminate this requirement. In order to improve the computation performance and reduce communication overhead, we propose a new verifiable outsourcing scheme with constant cipher text length. To be specific, our scheme achieves the following goals. (1) Our scheme is verifiable which ensures that the user efficiently checks whether the transformation is done correctly by the CSP. (2) The size of cipher text and the number of expensive pairing operations are constant, which do not grow with the complexity of the access structure. (3) The access structure in our scheme is AND gates on multivalued attributes and we prove our scheme is verifiable and it is secure against selectively chosen-plaintext attack in the standard model. (4) We give some performance analysis which indicates that our scheme is adaptable for various limited bandwidth and computation-constrained devices.

With the cloud service being more and more popular in modern society, ECC technology has become a promising orientation. It allows users to use flexible access control to access files stored in the cloud server with encrypted form. Though its advantages make it a powerful tool for cloud, one of its main performance challenges is that the complexity of decryption computation is linearly correlated with the access structure.

Given a cipher text and a transformation key, CSP transforms a cipher text into a simple cipher text. The user only needs to spend less computational overhead to recover the plaintext from simple cipher text. However, the correctness of the transformation cipher text which the CSP gives to the user cannot be guaranteed because the latter does not have the original cipher text. It is a security threat that malicious cloud service provider (CSP) may replace the original cipher text and give the user a transformed cipher text from another cipher text which CSP wants the user to decrypt.

The computational overhead for the decryption and transformation operations in our scheme is constant, which does not rely on the amount of attributes. In addition, we outsource the expensive operation to the cloud service provider and leave the slight operations to be done on user's device. Therefore, our scheme is very efficient.In proposed system, we implement asymmetric based encryption scheme to cloud services which is used to secure the data that are uploaded by user. This method practices two keys: public key and private key. The public key is made widely available and for secure data exchanging, receiver public key is used to encrypt data by sender. The private key is secret and is used to decrypt received encrypted data.

Encryption and decryption procedures using elliptic curves and they are described in the algorithms 1 and 2.

Algorithm 1: Elliptic Curve Encryption

```
Input: Parameters from the elliptic curve domain (p, E, P, n), Public Key Pk, Raw Text T
Output: Encrypted text (C1, C2) begin
1. Represent the message t as a point T in E(Fp)
2. Select k ∈R[1,n−1].
3. Calculate C1 = kP
4. Calculate C2 = T + kPk.
5. Return (C1, C2) end.
```

Algorithm 2: Elliptic Curve Decryption

```
Input: Parameters from the elliptic curve domain (p, E, P, n), Private key Sk, Encrypted text
(C1, C2) Output: Raw Text t begin
1. Calculate M = C2- dC1 and extract t from T.
2. Return (T). end.
```

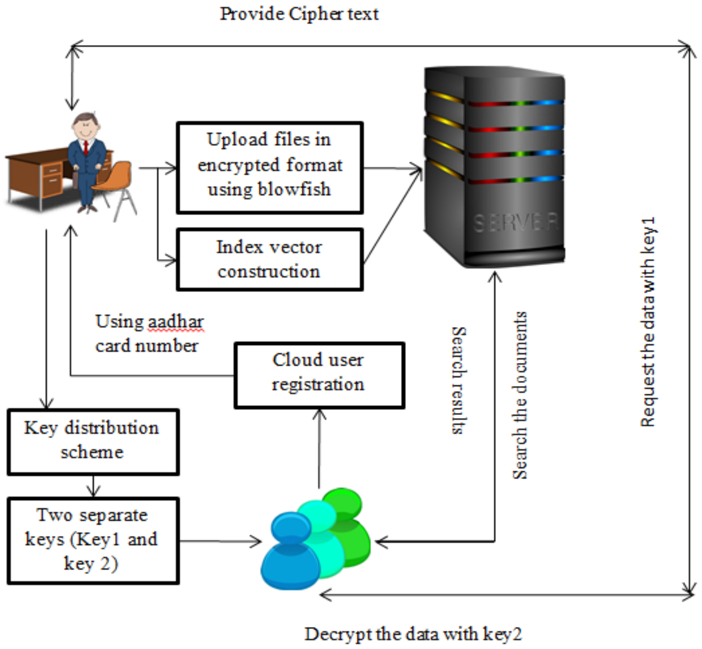

Provide Cipher text
Upload files in encrypted format using blowfish
Index vector construction
SERVER
Using aadhar card number
Cloud user registration
Search results
Search the documents
Request the data with key1
Key distribution scheme
Two separate keys (Key1 and key 2)
Decrypt the data with key2

Fig 4.1- Proposed work

V. CONCLUSION

In this paper, we tackled the challenging multi-keyword fuzzy search problem over the encrypted data. We proposed and integrated several innovative designs to solve the multiple keywords search and the fuzzy search problems simultaneously with high efficiency. In this approach of leveraging functions to construct the file index is novel and provides an efficient solution to the secure fuzzy search of multiple keywords. In addition, the fuzzy search is adopted to capture the similarity between the keywords and the secure inner product computation is used to calculate the similarity score so as to enable result ranking. We proposed a basic scheme as well as an improved scheme in order to meet different security requirements. We proposed a concrete scheme with verifiable outsourced decryption using a website for an IT firm to store and access documents and thereby proved that it is secure and verifiable. This scheme proved to be more efficient than existing approaches. This intermediate cipher text can be transformed into plaintext by proxy server. This process incurs a small computational overhead. Security of an ECC system with outsourced decryption ensures that an adversary (including a malicious proxy) will not be able to learn anything about the encrypted message; however, it does not guarantee the correctness of the transformation done by the cloud. We also consider a new requirement of ECC with outsourced decryption: verifiability. Thorough theoretical security analysis and experimental evaluation using real-world dataset were carried out to demonstrate the suitability of our proposed scheme for the practice usage.

REFERENCES

1. J. Tang, Y. Cui, Q. Li, K. Ren, J. Liu, and R. Buyya, “Ensuring security and privacy preservation for cloud data services,” ACMComputing Surveys, 2016.
2. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: Improved definitions and efficient constructions,” in Proceedings of the 13th ACM Conference on Computerand Communications Security. ACM, 2006, pp. 79–88.

3. W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," in Proceedings of the 8th ACMSIGSAC Symposium on Information, ser. ASIA CCS '13. ACM, 2013, pp. 71–82.
4. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEETransactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 222–233, 2014.
5. Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 2, pp. 340–352, 2016
6. W. M. Liu, L. Wang, P. Cheng, K. Ren, S. Zhu, and M. Debbabi, "Pptp: Privacy-preserving traffic padding in web-based applications," IEEE Transactions on Dependable and Secure Computing, vol. 11, no. 6, Nov 2014.
7. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in INFOCOM, 2010 Proceedings IEEE, 2010, pp. 1–5.
8. C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in Distributed ComputingSystems (ICDCS), IEEE 30th International Conference on, 2010, pp. 253–262
9. M. Chuah and W. Hu, "Privacy-aware bedtree based solution for fuzzy multi-keyword search over encrypted data," in DistributedComputing Systems Workshops (ICDCSW), the 31st International Conferenceon, 2011, pp. 273–281.
10. B. Wang, S. Yu, W. Lou, and Y. T. Hou, "Privacy-preserving multi-keyword fuzzy search over encrypted data in the cloud," in INFOCOM, 2014 Proceedings IEEE, 2014, pp. 2112–2120.

Securing an Image Using Arithmetic Coding and Hyper Chaotic Map

Mrs. D. Pauline Freeda
Associate Professor
Department of Computer Science and Engineering
St. Anne's College of Engineering and Technology

Ms.V.Sumitha, Ms.R. Sathya, Ms.M.Nathiya
UG Students
Department of Computer Science and Engineering
St. Anne's College of Engineering and Technology

Abstract - Recently, digital image processing is widely used in all aspects of human life, such as remote sensing, industrial inspection, medical field, meteorology, communications, reconnaissance, and intelligent robots. It is more important to protect the security of image data, especially in military, commercial, and medical fields. Due to the efficient and secure transmission of an image, we have to compress and encrypt the image. Image data own the characteristics of large amounts of data, strong correlations and high redundancy. The arithmetic coding and hyper chaotic map which are used to compress and encrypt image respectively. Before compression, shuffling the pixels of plain image is done. Arithmetic coding is used to compress the image into binary data and improves the compression ratio. It compresses the image row by row which is permuted by two logistic maps before arithmetic coding. Hyper chaotic map used to encrypt the binary data and improves the security of binary data. The different parameters and initial value for chaotic map is set. The compressed and encrypted image is secure and convenient for transmission.

Index Terms - **Image compression, image encryption, hyper chaotic map, arithmetic coding.**

I. INTRODUCTION

1.1. Image Encryption

Image encryption is the process of encoding an image in such a way that only authorized parties can access it and those who are not authorized cannot. Encryption does not itself prevent interference but denies the intelligible content to a would be interceptor. In an encryption scheme, the intended information or message, referred to as plaintext, is encrypted using an encryption algorithm, a cipher generating cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, considerable computational resources and skills are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients but not to unauthorized users.

In military, commercial, and medical fields images are keep in more secure. Because of image has the characteristics of large amounts of data, strong correlations, and high redundancy, it needs to be transmitted safely over the network. It should be protected without worried about intercepted and captured. An image cannot be hacked easily, if it is in unrecognized format using strong image encryption algorithm. To secure an image to compress and encrypt using arithmetic coding and hyper chaotic map. First plain image is shuffled by pixels of image and compress the shuffled image using arithmetic coding. Then encrypt the compressed image using hyper chaotic map. It is more secure during an image transmission. Images are widely used in different areas nowadays this project ensures the limitation of unauthorized access and provide better security during image transmission. Secured image can be used in various fields such as medicals diagnosis, commercial, military and securing government documents.

- Internet multimedia application
- Medical image encryption
- Picture messaging on cell phone
- Securing government document
- Military

1.2. Chaotic System

"Chaos" means "a state of disorder". Chaotic systems have initial value sensitivity, pseudo randomness, and non periodicity, which are consistent with the characteristics required for cryptography. The confusion and diffusion structure of image encryption algorithms is based on chaotic systems for the use of chaotic sequences, and it is restricted by the computer word length, which can cause degradation in the chaotic dynamics, especially for a low-dimensional chaotic system. This limitation seriously affects the security of the chaotic encryption.

1.3. Hyper Chaotic System

Hyper chaos systems to ensure the complexity of the chaotic sequence, to improve the security of the encryption algorithm. Compared with a low-dimensional chaotic system, high-dimensional chaotic systems have a more positive Lyapunov exponent and are more complex, and it is more difficult to predict the dynamic characteristics, which can effectively solve the degradation problem of the low-dimensional chaotic system with dynamics characteristics. It also has strong confidentiality, a simple algorithm, and large key space characteristics.

1.4. Arithmetic Coding

Arithmetic coding is a form of variable length entropy encoding used in lossless data compression. Entropy encoding uses the shortest codes to encode the most common symbols. It differs from other form of entropy encoding in that rather than separating the input into component symbols and replacing each with a code arithmetic coding encodes entire message into a single number. The advantage of arithmetic coding over other similar methods of data compression is the convenience of adaptation.

II. LITERATURE SURVEY

Xiang, Wang, Yinfa, Ping proposed an improvement colour image encryption algorithm based on DNA operations and real and complex chaotic systems. It is done by hyper chaos

Lorenz system and it using wavelet function. It improves the ability of resisting differential attacks by using Hamming distance and one-time pad to generate the secret keys. The numerical simulations and security analysis show that the proposed algorithm has better encryption effect, larger secret key space and higher sensitive to the secret key.

Wong, Ling and Chen proposed Simultaneous Arithmetic Coding and Encryption Using Chaotic Maps for compression and encryption scheme. The average percentage of bits changed in the cipher text sequences varies from 46.13% to 49.96% and is very close to the ideal value (50%). It is only encrypting the text format.

Danial and Yaghoobi proposed Colour Image Encryption using Hyper Chaos Chen. It is done by Arnold mapping and Hyper chaos Chen system to encrypt the colours red, green and blue pixels are all cluttered image. This outcome image is not clear in decryption modules. It has loss of image encryption.

Huang, Yuxia and Jinling proposed a Colour Image Encryption algorithm based on a Fractional order hyper chaotic system for generating four chaotic sequence. The plain image is encrypted by performing the XOR and shuffling operations simultaneously. The histograms of the encrypted image are slightly uniform . So they do provide any clues that could be employed for any statistical analysis attack on the encrypted image.

Tiegang Gao and Zengqiang Chen proposed a new image encryption algorithm based on hyper chaos using an image total shuffling matrix to shuffle the positions of image pixels and then uses a hyper chaotic system to confuse the relationship between the plain-image and the cipher image. The key space is less large so possible to make brute-force attacks.

III. EXISTING SYSTEM

In existing system an image is compressed and encrypt by using arithmetic coding and chaotic map. The key is divided into four parts as the parameters and initial value of logistic maps. In order to let the key relate to plain-image, the pixels of plain image are first made in sets of sixteen from top to bottom and left to right, namely 128 bits in one set. Then, generate the chaotic sequence after image is row by row permuted by two logistic maps. The chaotic sequences are expressed in descending numerical order. This order is used to permute the rows of plain image only once, namely shuffling the order of rows. After permutation , an image is compressed by arithmetic coding and the compressed image is transformed into binary data. Then chaotic sequences are transformed into binary data. The compressed binary data of every row is diffused by binary chaotic sequence using XOR operation.

IV. PROPOSED SYSTEM

In proposed system, a plain image is divided. Then shuffle the position of divided image and the pixels of divided image. Then compression is done using Arithmetic coding and encryption is done using hyper chaotic map. Compression is done by row by row pixel of image. Hyper chaotic has four key sequences to encrypt the compression image. If there is little change in key sequence while decryption process, it will major changes in decrypted image. This system is not possible to hack the image while transmission.

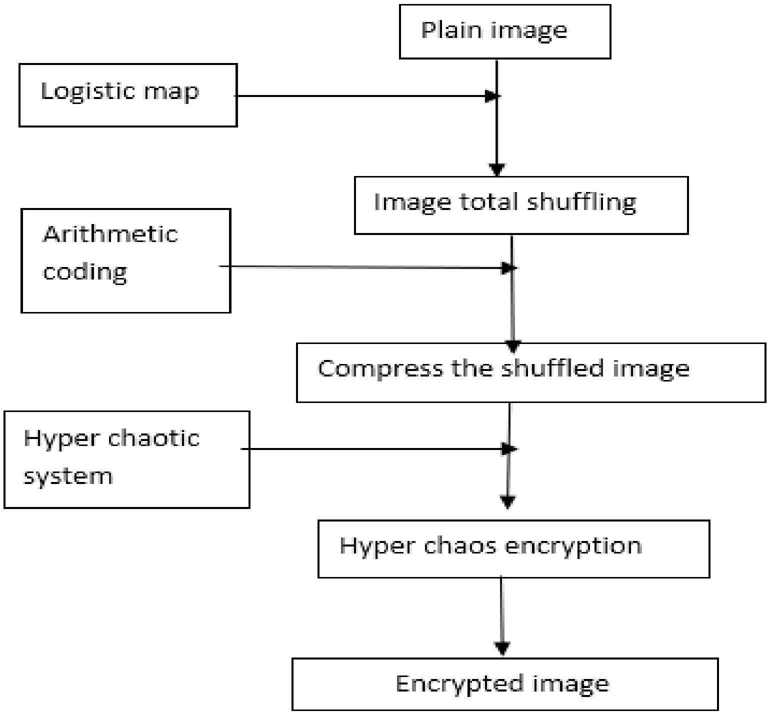


Figure 4.1 - Block diagram of Proposed system

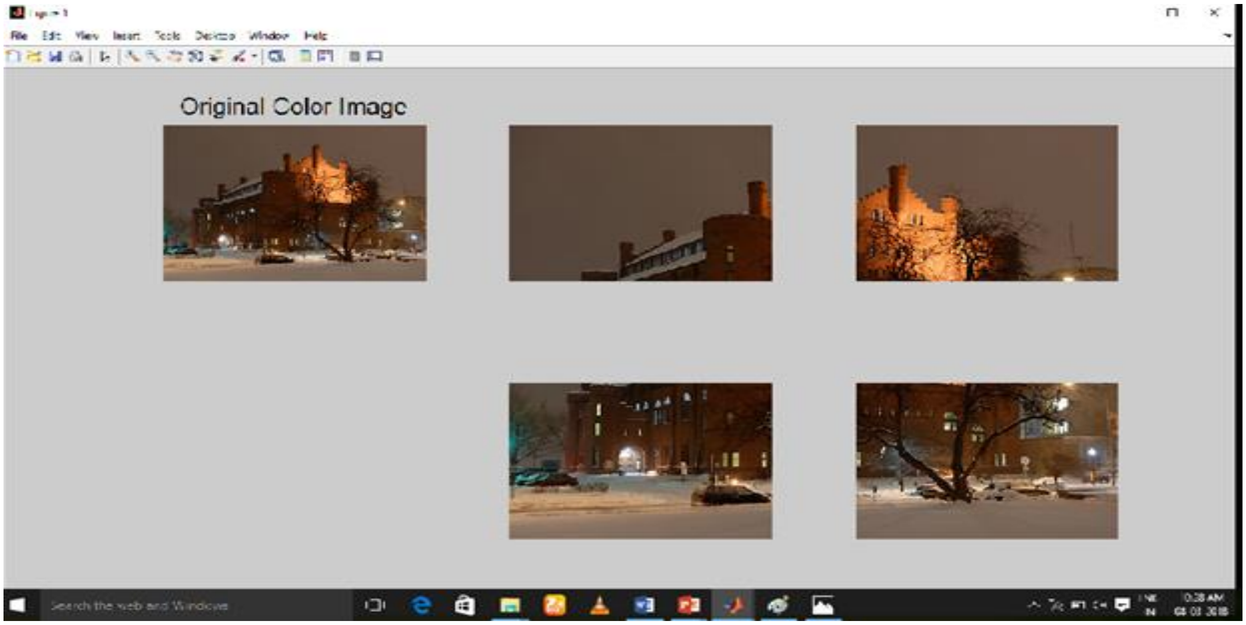

File Edit View Insert Tools Desktop Window Help
Original Color Image
Search the web and Windows

Fig 4.2 - Divided image

Fig 4.3 - Ciphered image

V. CONCLUSION AND FUTURE ENHANCEMENT

An image is secured using arithmetic coding and hyper chaos for transferring an image in a network. The plain image is compressed and encrypted by arithmetic coding and hyper chaotic map. The hyper key sequences are strong and more secure. It is not possible to hack the key sequence because it key sensitivity. So it can be concluded that hyper chaos encryption algorithm is sensitive to the key, a small change of the key will generate a completely different decryption result and cannot get the correct plain-image.

An image can be secure using Huffman coding for compression and Hyper chaos for encryption in future. Because Huffman coding is variable entropy encoding for image cryptology. Huffman coding easy to generate encryption key and reduce the key generating time. Thus an image can be secured by Huffman coding and Hyper chaos system.

REFERENCES

1. G. Chen, et al., A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos Solitons Fractals 21 (3) (2004) 749–761.
2. S. Lian, et al., A block cipher based on a suitable use of the chaotic standard map, Chaos Solitons Fractals 26 (1) (2005) 117–129.
3. Y. Wang, et al., A chaos-based image encryption algorithm with variable control parameters, Chaos Solitons Fractals 41 (4) (2009) 1773–1783.
4. Y. Wang, et al., A new chaos-based fast image encryption algorithm, Appl. Soft Comput. 11 (1) (2011) 514–522, http://dx.doi.org/10.1016/j.asoc.2009.12.011.
5. K.W. Wong, C.H. Yuen, Embedding compression in chaos-based cryptography, Circuits Syst. II: Express Brief. IEEE Trans. 55 (11) (2008) 1193–1197.
6. K.W. Wong, et al., Simultaneous arithmetic coding and encryption using chaotic maps, Circuits Syst. II: Express Brief. IEEE Trans. 57 (2) (2010) 146–150.
7. R. Bose, S. Pathak, A novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system, Circuits Syst. II: Express Brief. IEEE Trans. 53 (4) (2006) 848–857.

Augmentation of Network Security in Open Flow Structure Using Software Defined Networking

Ms.S.Vanathi
Assistant Professor,
Department of Computer Science and Engineering,
St. Anne's College of Engineering and Technology,

Ms. R.Leema Roseline, Ms. R.Nishanthi,
UG Students,
Department of Computer Science and Engineering,
St.Anne's College of Engineering and Technology,

Abstract - Software defined networking is a computer networking by using a open flow protocol. To provide a security measure in a opensec in Software Defined Networking (SDN) atmosphere for mischievous node reacts to a opensec protocol. In this the communication between the switch and controller and requested node in a network. The main objective is to give priorities on the basis of trust level, then according to that it will handle the request. And to keep the control plane in running state efficiently even when suffering from data-to-control plane saturation by assigning less timeout value for the flow rule in peak time. The secondary objective is to differentiate between counterfeit packet request from normal packet request and it handles the data-to-control plane saturation. The performance metric is evaluated by using the number of packet loss and its time taken for its communication.

Index Terms **- Software defined network, openflow, security, attack detection, secured data.**

I. INTRODUCTION

Thus they are various security issue has been occurred in the openflow in software defined network environment. In a flow table notification relocation in environment thus the data allocation between the controller, switch and with the requested node to transfer the data. And it based on the functionality of an abstraction of lower level in the environment. Since there is no extent to afford security in the open flow flow table messages. To improve a security issue first to process the bunching to the neighbor node and dissemination is performed. And it develops the computational of scalability and it immobile in position. Thus it process a decoupling the node in a synchronization that make to perform a verdict making that which node to proceed. And the data transfer in flow table communications is between the control and the receiver as implored node transfer.Thus the process involved with a open flow protocol for the purpose of sequestered data communication and to select the path between the lattices controls.

Thus the processes of security disputes and the spasms present in software defined networks are as data outflow when more numbers of node entreated from the packet while transmitting data .It causes a denial of services, reviewed data while conveying the when attacker hack the data in a node. Attacks on evolving data plane embraces in DOS are control dos, complex dos, TCAM breakdown, switch back hole.

In existing work, they complete only in the site network environment by using a OpenSec in a software defined state, where security charter is based on openflow . And security strategy is written in a human readable language which is instigated in a network security operator that allows a network security operator. The security measures are realistic to its field, using opensec such as attacks In this work the security policy will responds to opensec if the malicious node traffic is found detected. And it passes a openflow message to opensec when a mischievous nodes is perceived to the controller in a network. In a campus network they use a dataset to evaluate the security and the scalability issues by performing the testbed as GENI to detect the spasms and the malicious node present in the network in which it blocks inevitably as 95%of attacks and the 97% of source of malicious node in surroundings network.

In a proposed work , the ingesting of nodes are accomplished and the neighbor fragment acquaintance is performed. And the statistics declaration in flowtable missive is done between the modification and resistor and with the entreated nodes. First it process done by bundling is done by using AOMDV (On-demand Multipath Distance Vector Routing in Ad Hoc Networks) in this every single node will preserve the series number to track the node and it update the way value by RREQ and RREP for a path progressing in node .and it procedures a cloudwatcher procedure the perceive and wedge the attacks before it hacks the data while spreading .attacks which include gray scale attacks and dos attacks in controller. Finally it spots the malicious nodes such as selfish node are professed and it updates the secure data update in the reliable flow table transmission.

II. RELATED WORK

This section briefly review earlier works based on the security issue in open flow framework. A number of approaches have been reported in the literature survey for security measure and block of attacks and the malicious nodes.

Adrian Lara and Byrav Ramamurthy in their work they propose a Network-aware controller handles the configuration of all network devices. Software applications running on top of the network controller provide an abstraction of the topology and facilitate the task of operating the network. We propose OpenSec, an OpenFlow-based security framework that allows a network security operator to create and implement security policies written in human-readable language. Using OpenSec, the user can describe a flow in terms of OpenFlow matching fields, define which security services must be applied to that flow (deep packet inspection, intrusion detection, spam detection, etc.) and specify security levels that define how OpenSec reacts if malicious traffic is detected.

Jiaqiang Liu Yong Lia and Huandong Wang they have addressed the problem in Network operators to employ a variety of security policies for protecting the data and services, deploying these policies in traditional network is complicated and security vulnerable due to the distributed network control and lack of standard control protocol. We introduce a safe way to update the configuration of these switch one by one for better load balance when traffic distribution changes. The update process as a path in a graph, in which each node represents a security policy satisfied configuration, and each edge represents a singles safely update. Based on this model, we design a heuristic algorithm to find an optimal update path in real time. Simulations of the update scheme show that our proposed algorithm is effective and robust under an extensive range of conditions. The Dijkstra algorithm can be used to find the shortest path from the initial state to the destination state.

Bing Xiong., Kun Yang., Jinyuan Zhao., Wei Li and Keqin Li in this work they discussed about the Performance evaluation security issues in OpenFlow-based software-defined networks based on queueing model in OpenFlow is one of the most famous protocols for controller-to-switch communications in software-defined networking (SDN), commonly seen as a promising way towards future Internet. Understanding the performance and limitation of OpenFlow-based SDN is a prerequisite of its deployments. To achieve this aim, this paper proposes a novel analytical performance model of OpenFlow networks based on queueing theory.

Changhoon Yoona. Taejune Parka. Seungsoo Leea and Zonghua Zhang addressed the problem inEnabling security functions with SDN In this paper, we verify whether SDN can enhance network security. Specifically, the idea of enabling security function with diverse SDN features is explored thoroughly. In order to elucidate the feasibility of SDN based security functions, such as a In line mode security function as firewalls and IPS, passive mode security functions as IDS), network anomaly detection functions as scan and DDoS detector advanced security functions a stateful firewall and reflector networks.

WenjuanLi., WeizhiMeng and LamForKwok they discussed Security challenges and countermeasures has been proposed as an emerging network architecture, which consists of decoupling the control planes and data planes of a network. Due to its openness and standardization, SDN enables researchers to design and implement new innovative network functions and protocol in a much easier and flexible way. In particular, OpenFlow is currently the most deployed SDN concept, which provides communication between the controller and the switches. However ,the dynamism of programmable networks also brings potential new security challenges relating to various attacks such as scanning, spoofing attacks, denial-of-service(DoS) attacks and soon.

Xiulei Wang., Ming Chen., and Changyou Xinghas described about the Software-Defined Security Networking Mechanism to Defend against DDoS Attacks. The Distributed Denial of Service (DDoS) attack has seriously harmed network availability over decades and there is still no effective defense mechanism. The emerging software defined networking (SDN) gives a new way to rethink the defense of DDoS attacks. In this paper, we first modeled DDoS attacks from the perspective of network architecture. Then a software defined security networking mechanism was proposed to remove or restrict these necessary conditions which were summarized from the model.

Saksit Jantila and Kornchawal Chaipah they discussed about A Security Analysis of a Hybrid Mechanism to Defend DDoS Attacks in SDN. In this paper, we propose adapting a hybrid mechanism against DDoS attacks from the traditional network for SDN. The mechanism relies on trust values and entropy based on clients' access behaviors. We identify threats to this application and suggest use of existing SDN's and our proposed mechanisms to prevent and mitigate the threats. Moreover, authentication, encryption, and the use of public/private keys play important roles in keeping entities in SDN safe from attackers. In the future, we plan to implement and simulate the proposed mechanism in a virtual SDN to assess the mechanism's effectiveness and efficiency, and to identify any flaws we might have overlooked.

Javed Ashraf and Seemab Lati has come with system of handling the security measure in Intrusion and DDoS Attacks in Software Defined Networks Using Machine Learning Techniques This paper aims at studying SDN accompanied with OpenFlow protocol from the perspective of intrusion and Distributed Denial of Service (DDoS) attacks and suggest machine learning based techniques for mitigation of such attacks. the critical security threats of SDNs and in augmenting its security such as classifying applications and using rule prioritization, to ensure that rules generated by security applications will not be overwritten by lower priority applications.

III. PROPOSED WORK

The proposed system has Main detached is to give priorities on the basis of confidence level, then affording to that it will handle the request .The prime objective is to keep the control plane in running state proficiently even when suffering from data-to-control plane overload by assigning less timeout value for the flow rule in peak time. The secondary objective is to differentiate between fake packet application and normal packet request handles the data-to-control plane.

A controller in statement will manages data input and output to a computer in a host network and it perform the all the indispensible control functions, error checking, and harmonization. The flow table will update the most recent devices perform data inflexibility, route selection, security functions, and collect executive information. Manage data communication over message associates and control the flow of data with the switch and the controller with respective host in nodes.

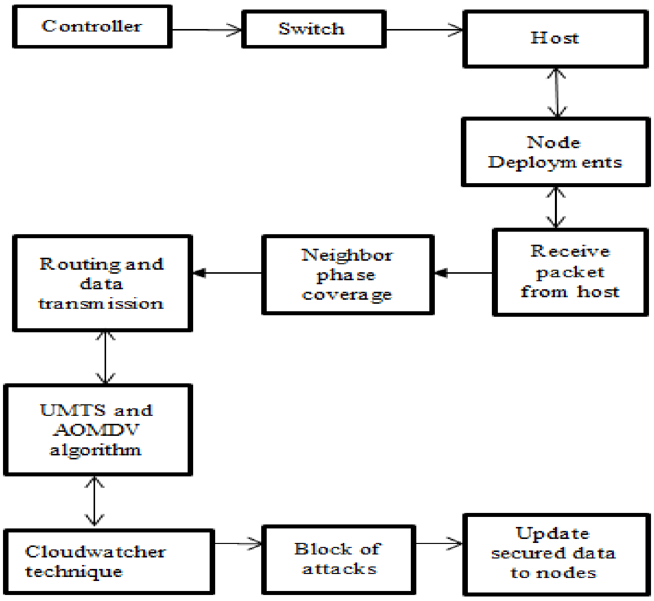


Fig 3.1 System Architecture

It performs

- Essence cluster controller networks, and poll those controls to see if they have data to transmit
- Refuge arriving or outgoing data
- Identify and correct errors
- Provide overthrowing functions to get data to its target.

The Modules of the proposed systems are:

- Node deployment and neighbor segment coverage
- Routing and Data diffusion
- Malevolent host detection
- Block of attackers and Inform Secured data

3.1 Node Deployment And Neighbor Segment Coverage

Node exploitation is the initial stage for the flow table message announcement. In flow table there will be many attackers and the malicious node will be presented. For such purpose first the nodes must be deployed and the clustering process as it broadcast as neighbor phase coverage in software defined network situation. In the deployment process thus nodes as host moves frequently it act as a end point and forward packet routers in the transmission source range of multi hop environment. The topology of networks changes unpredictably. By organizing the node thus the manifestation of new nodes might be transpired in the neighbor phase coverage.

- ➢ Packet delivery ratio augmentations.
- ➢ Decrease in the average end -to -end delay Diffusions.
- ➢ Nonaggressive in Repeated link breakages and conduit failures leads to virtuous vast concert when the network is in extraordinary hardness.

3.2 Routing and Data Diffusion

In a routing and data broadcast it involves the clustering process it involves AOMDV algorithm .It maintain its own invariant sequence of its own destination numbers. In this Routing host will move from one packets to another across a networks. While transmitting it increases the Packet switching efficiency network, robustness. Thus the Packets of nodes has the header and payload. Each packet is then transmitted individually in same path or might be in different path to its destination. In a flow table if all of the packets has reached at the destination, they automatically reconvened to recreate the original message.

An attacker in a malicious node to hack the data while transmitting the data in the flow table target system to prevent authentic access. Cloud watcher, which provides observing facilities for large and active cloud networks. This framework automatically detours network packets to be inspected by pre-installed network security devices.

AOMDV(On-demand Multipath Distance Vector Routing in Ad Hoc Networks) Routing Algorithm:

The node discoveries its own address among the addresses listed in the message and it informs the current status of the data transmission and the neighbor property time in a controller. If the node does not treasure its own address among the addresses listed in the broadcast message it broadcast again the another neighbor nodes in the host address. By using the gathering process it broadcast the messages.

3.3 Malevolent Host Detection

In a malevolent host detection it uses the cloudwatcher technique in the flow table transmission where the requested nodes is needed to transmit the dispatch,by using the cloud watcher technique the attackers and the malevolent node is detected.

3.4 Cloudwatcher Technique

Cloud watcher technique is a technique is used to observer the network security in the software defined network environment using openflow in opensec structure. it security to the controls of network flows to the security devices of all packets.

(i) And it increase the efficient strategy scripting language to provide security and services easily.

(ii) In a flowtable the transmission between the controller and host the cloudwatcher can easily variations the path of routing network flows, and it makes the flows transmit through network nodes where retreat devices reside.

3.5 Block Of Attacks And Update Secured Data

In this development after detection and block of malicious host secured data update and the graphical results of the attacker has been blocked in a network. Since they exist a selfish node in a flow table in a software well-defined network environment and the gray scale attack has been distinguished while in the data transmission in the nodes. And it provides a Secured data protects the processing and storage of code using encryption, fault and management detection, and secure code and data storage.

The open dispute attacks are:

- Unauthorized Modification Using Uniqueness Spoofing Attacks
- Flooding Attacks
- Man in middle attack
- Eavesdropping
- DDOS attack
- ARP spoofing
- Side-channel attacks

Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator and controller update the flow table.

IV. EXPERIMENTAL ANALYSIS

NS2 is an open-source recreation tool that turns on Linux. It is a discreet event simulator directed at networking research and provides important support for repetition of routing, multicast conventions and IP protocols, such as UDP, TCP, RTP and SRM over wired and wireless networks. It has many advantages that make it a useful tool, such as support for numerous protocols and the ability of explicitly detailing link traffic. The nodes are free to move randomly and act as end sockets as well as routers to advancing packets in a multi-hop setting where all nodes may not be within the transmission range of the source. Decrease in the average end delay Transmissions. Attack has been detected and identify the malicious host and affords the security measure in it. And the controller updates the flow table messages to the switch movement and provides the trusted data information to the needed node.

V. RESULT ANALYSIS

For evaluating the performance of compatible technique and approaches, And the concert exploration is based on the packet loss, amount, and acknowledgment of attacks with malicious nodes and deprived of attacks based upon the throughput.

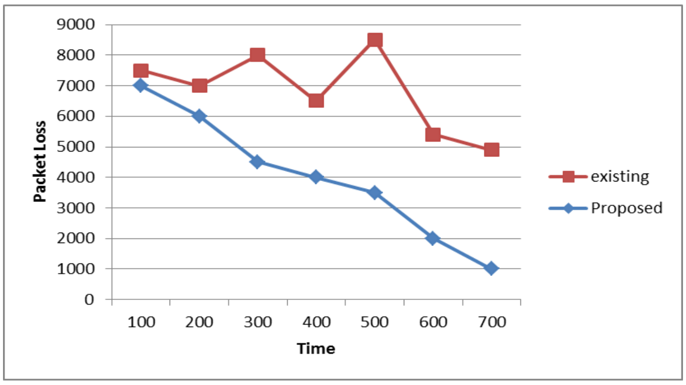


Fig 5.1 Packet Loss

Packet loss is calculated by

Packet loss = Total number of transmitted packet

Total Number of received packet.

Packet transmission time = Total number of Packet size

Bit rate

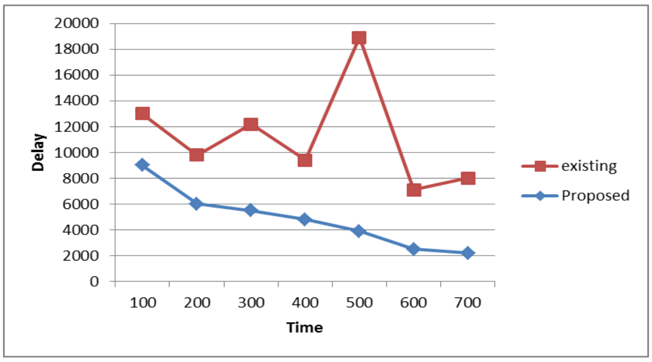


Fig 5.2 Througput (Time vs Delay)

Throughput= file size/ broadcast Time.

Broadcast time is calculated by the broadcast time, is the sum of time from the creation until the end of a missive spread. In the case of a numeral message, it is the time from the first bit until the last bit of a message has left the transmitting node.Since the gathering process is performed and the cloud watcher method is efficient to route and cluster the node deployment with the network realization. By data transmitting it uses the UMTS process for transmit and for routing process. And after the completion of process in routing and transmission it enables the attack uncovering technique and block of extraneous data and the attacks present in the open flow. It process and update the protected data in the software defined network environment.

VI. CONCLUSION

The project evaluate the various security concern in a data communication and data routing by using the broadcasting the neighbor nodes using control, switches and host. In a OpenFlow-based structure that allows network operators to describe security policies controller and automatically converts security policies into a set of rules that are pushed into network devices. OpenSec also allows network operators to specify how to automatically react when malevolent traffic is detected. It allows for automated reaction to security alerts based on pre-defined system policies. The analysis of traffic away from the controller and into the dispensation units makes our framework more scalable. An attack detection trigger method was for the first time presented to agenda the starting of attack enlightening. An attack detection method was used to discover the attack. A system the trigger mechanism of the attack detection implemented on controller. In security fixed routing, a routing protocol can act as a exporter that helps not only in guiding the traffic but also in defensive it. Security controls permit deny traffic based on network level information IP, port number or protocol.

REFERENCES

1. Adrian Lara and Byrav Ramamurthy "OpenSec: Policy-Based Security Using Software-Defined Networking"IEEE transactions on network and service management, (2016)Vol. 13, No. 17.

2. Bing Xiong., Kun Yang., Jinyuan Zhao., Wei Li and Keqin Li "Performance evaluation security issues in OpenFlow-based software-defined networks based on queueing model". In Proceedings of the European Workshop on Software Defined Networks (EWSDN),Germany, (2014) ACM .Vol 26 ; pp. 91–96.

3. E. Bertino "Analysis of privacy and security policies", J. Res. Develop., (2009) ACM Vol. 53, No. 2, pp. 3:1–3:18.

4. ChanghoonYoona., TaejuneParka., SeungsooLeea., and ZonghuaZhang "Enabling security functions with SDN". Computational. Communication. (2015) ACM Vol 38, pp 69–74.

5. Javed Ashraf and Seemab Latif "Handling security measure in Intrusion and DDoS Attacks in Software Defined Networks Using Machine Learning Techniques". (2014)IEEE Transaction. Network. Service Manage., Vol. 12, No. 1, pp. 48–60.

6. JiaqiangLiu.,YongLia., and HuandongWang "Leveraging software defined networking for security policy enforcement". Communication computation. China, (2015) Vol. 11, No. 78, pp. 45–55.

7. Lara and B. Ramamurthy "OpenSec: A framework for implementing security policies using OpenFlow " in Procera. Globecom Conf., Austin, TX, USA, (2014) IEEE Vol 34, No.67 pp. 781–786.

8. D. Li, X. Hong, and J. Bowman "Evaluation of Security Vulnerabilities by Using ProtoGENI" as a Launchpad, (2015),IEEE, pp. 1–6.

9. Mohan Dhawan, Rishabh Poddar, Kshiteej Mahajan, and Vijay Mann " SPHINX: Detecting Security Attacks in Software- Defined Networks." (2015) .ACM. pp. 21:1–21:6

10. S. Shin and G. Gu "Attacking Software-Defined Networks The First Feasibility Study,in Proceedings of the second ACM SIGCOMM workshop in software defined networking". (2013) ACM, 2013,Vol .67 pp. 160–166.

11. R. Smeliansky"SDN for network security,in Science and Technology International". (2014) IEEE, Vol 34-65,No.23, pp. 1–5.

12. Saksit Jantila and Kornchawal Chaipah "A Security Analysis of a Hybrid Mechanism to Defend DDoS Attacks in SDN". Communication. system(2014)IEEE Vol 51, pp.128–134.

13. S. Shin, P. A. Porras, V. Yegneswaran, M. W. Fong, G. Gu, and M. Tyson. Fresco: Modular composable security services for software-defined networks. (2013) ACM. pp. 21:1–21:6.

Ciphertext ABE Algorithm to Fix De-Duplication in Amazon Cloud

P. Keerthana, R. Revathy, P. Sangeetha,
UG Students
Department of Information Technology,
Anand Institute of Technology, Kazhipathur.

Shobhanjaly P Nair,
Assistant Professor
Department of Information Technology,
Anand Institute of Technology, Kazhipathur.

Abstract - Attribute-based encryption (ABE) has been widely used in cloud computing where a data provider outsources his/her encrypted data to a cloud service provider and can share the data with users possessing specific credentials (or attributes). However, the standard ABE system does not support secure deduplication, which is crucial for eliminating duplicate copies of identical data in order to save storage space and network bandwidth. In this paper, we present an attribute-based storage system with secure deduplication in a hybrid cloud setting, where a private cloud is responsible for duplicate detection and a public cloud manages the storage. Compared with the prior data deduplication systems, our system has two advantages. Firstly, it can be used to confidentially share data with users by specifying access policies rather than sharing decryption keys. Secondly, it achieves the standard notion of semantic security for data confidentiality while existing systems only achieve it by defining a weaker security notion. In addition, we put forth a methodology to modify a cipher text over one access policy into cipher texts of the same plaintext but under other access policies without revealing the underlying plaintext.

Index Terms - **cipher text-attribute based encryption algorithm, equality checking algorithm, Huffman technique.**

I. INTRODUCTION

The concept of deduplication is to eliminate the redundant data. We provide definitions of privacy and integrity peculiar to this domain. Now having created a clear, strong target for designs, we make contributions that may broadly be divided into two parts: practical and theoretical. We analyze existing schemes and new variants, breaking some and justifying others with proofs in the random-oracle-model (ROM). MLE emerges as a primitive that combines practical impact with theoretical depth and challenges, making it well worthy of further study and a place in the cryptographic pantheon. Below we begin with some background and then look more closely at our contributions.

Many enterprises and other organizations need to store and compute on a large amount of data. Cloud computing aims at renting such resources on demand. Cloud providers offer both, highly available storage and massively parallel computing resources with High Performance Computing (HPC) at low costs, as they can share resources among multiple clients.

Several attribute-based constructions have been presented. A common classification property is whether a system is a "small universe" or "large universe"constructions. In"small universe"constructions the size of the attribute space is polynomially bounded in the security parameter and the attributes were fixed at setup. Moreover, the size of the public parameters grew linearly with the number of attributes. In "large universe" constructions, on the other hand, the size of the attribute universe can be exponentially large, which is a desirable feature.

A technique which has been proposed to meet these two conflicting requirements is convergent encryption whereby the encryption key is usually the result of the hash of the data segment. Although convergent encryption seems to be a good candidate to achieve confidentiality and deduplication at the same time, it unfortunately suffers from various well-known weaknesses including dictionary attacks: an attacker who is able to guess or predict a file can easily derive the potential encryption key and verify whether the file is already stored at the cloud storage provider or not.

CLF is a new emerging field of data security used to analyzed at a inside cloud log files for the investigation of malicious behaviour. However, cloud log files are only accessible to a Cloud Service Provider (CSP) through cloud resource ownership. For instance, in cloud computing Software-as-a-Services (SaaS),a user is provided with developed software to run its applications. Each application generates log files during its execution on the cloud that are inaccessible to the users [Ruan et al. 2011].

II. LITERATURE REVIEW

2.1 Message-Locked Encryption And Secure Deduplication

We formalize a new cryptographic primitive, Message-Locked Encryption (MLE), where the key under which encryption and decryption are performed is itself derived from the message. MLE provides a way to achieve secure deduplication (space-efficient secure outsourced storage), a goal currently targeted by numerous cloud-storage providers. We provide definitions both for privacy and for a form of integrity that we call tag consistency. Based on this foundation, we make both practical and theoretical contributions. On the practical side, we provide ROM security analyses of a natural family of MLE schemes that includes deployed schemes. On the theoretical side the challenge is standard model solutions, and we make connections with deterministic encryption, hash functions secure on correlated inputs and the sample-then-extract paradigm to deliver schemes under different assumptions and for different classes of message sources. Our work shows that MLE is a primitive of both practical and theoretical interest.

2.2 Security Proofs For Identity-Based Identification And Signature Schemes

This paper provides either security proofs or attacks for a large number of identity-based identification and signature schemes defined either explicitly or implicitly in existing literature. Underlying these are a framework that on the one hand helps explain how these schemes are derived, and on the other hand enables modular security analyses, thereby helping to understand, simplify and unify previous work.

2.3 Gq And Schnorr Identification Schemes: Proofs Of Security Against Impersonation Under Active And Concurrent Attacks

The Guillou-Quisquater (GQ) and Schnorr identification schemes are amongst the most efficient and best-known Fiat-Shamir follow-ons, but the question of whether they can be proven secure against impersonation under active attack has remained open. This paper provides such a proof for GQ based on the assumed security of RSA under one more inversion, an extension of the usual onewayness assumption that was introduced in. It also provides such a proof for the Schnorr scheme based on a corresponding discrete-log related assumption. These are the first security proofs for these schemes under assumptions related to the underlying one-way functions. Both results extend to establish security against impersonation under concurrent attack

2.4 Twin Clouds: An Architecture For Secure Cloud Computing

Cloud computing promises a more cost effective enabling technology to outsource storage and computations. Existing approaches for secure outsourcing of data and arbitrary computations are either based on a single tamper-proof hardware, or based on recently proposed fully homomorphic encryption. The hardware based solutions are not scaleable, and fully homomorphic encryption is currently only of theoretical interest and very inefficient. In this paper we propose an architecture for secure outsourcing of data and arbitrary computations to an untrusted commodity cloud. In our approach, the user communicates with a trusted cloud (either a private cloud or built from multiple secure hardware modules) which encrypts and verifies the data stored and operations performed in the untrusted commodity cloud. We split the computations such that the trusted cloud is mostly used for security-critical operations in the less time-critical setup phase, whereas queries to the outsourced data are processed in parallel by the fast commodity cloud on encrypted data.

2.5 Reclaiming Space From Duplicate Files In A Serverless Distributed File System

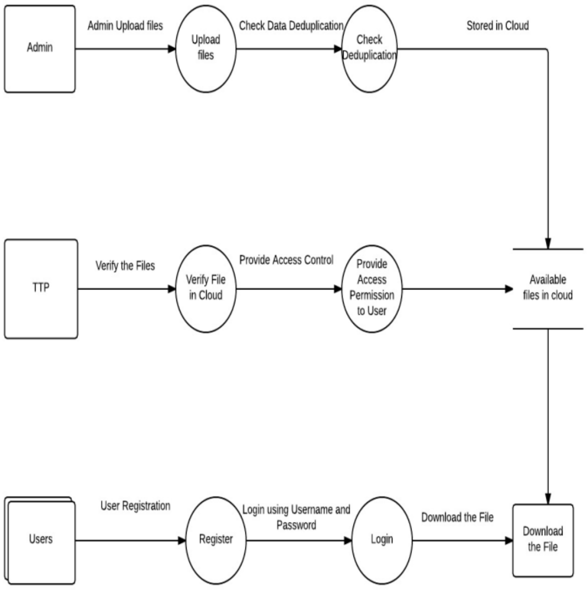
The Farsite distributed file system provides availability by replicating each file onto multiple desktop computers. Since this replication consumes significant storage space, it is important to reclaim used space where possible. Measurement of over 500 desktop file systems shows that nearly half of all consumed space is occupied by duplicate files. We present a mechanism to reclaim space from this incidental duplication to make it available for controlled file replication. Our mechanism includes 1) convergent encryption, which enables duplicate files to coalesce into the space of a single file, even if the files are encrypted with different users' keys, and 2) SALAD, a SelfArranging, Lossy, Associative Database for aggregating file content and location information in a decentralized, scalable, fault-tolerant manner. Large-scale simulation experiments show that the duplicate-file coalescing system is scalable, highly effective, and fault-tolerant.

III. PROPOSED SYSTEM

We present an attribute-based storage system which employs cipher text-policy attribute-based encryption (CPABE) and supports secure deduplication. In this paper, we proposed Equality Checking Algorithm to check the files/data whether it's duplicate or not. Any duplication files present it will intimate to data owner. The Symmetric Algorithm is used to encrypt the files/data for security purpose and this project implemented for AmazonS3 Cloud. In other hand, Huffman technique is used to compress the size of file so, the storage space optimized in cloud.

IV. IMPLEMENTATION

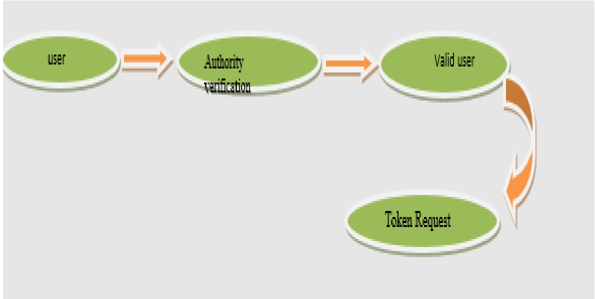
In this new deduplication system, a hybrid cloud architecture is introduced to solve the problem. The private keys for privileges will not be issued to users directly, which will be kept and managed by the private cloud server instead. In this way, the users cannot share these private keys of privileges in this proposed construction, which means that it can prevent the privilege key sharing among users in the above straightforward construction. To get a file token, the user needs to send a request to the private cloud server. The private cloud server will also check the user's identity before issuing the corresponding fill token to the user. The authorized duplicate check for this file can be performed by the user with the public cloud before uploading this file. Based on the results of duplicate check, the user either uploads this file or runs POW.



This paper contains the following modules:

4.1 Authorization control creation and Key Generation

The private keys for privileges will not be issued to users directly, which will be kept and managed by the private cloud server instead. In this way, the users cannot share these private keys of privileges in this proposed construction. The privilege key sharing among users in the above straightforward construction. To get a file token, the user needs to send a request to the private cloud server.

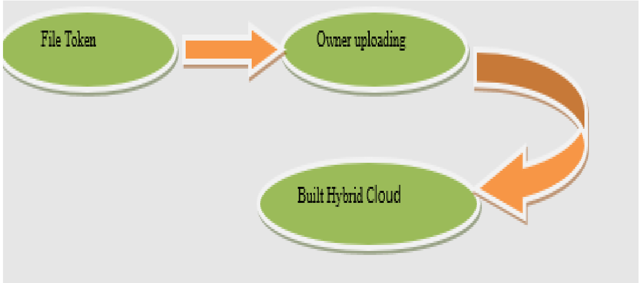


Setup(λ,U). The setup algorithm takes security parameter and attribute universe description as input. It outputs the public parameters PK and a master key MK.

Key Generation(MK,S). The key generation algorithm takes as input the master key MK and a set of attributes S that describe the key. It outputs a private key SK.

4.2 Owner Uploading and Built Hybrid Cloud

A user can upload a file and stored in a private cloud. The private keys for privileges will not be issued to users directly, which will be kept and managed by the private cloud server instead.In users cannot share these private keys of privileges in this proposed construction. The privilege key sharing among users in the above straightforward construction.The authorized duplicate check for this file can be performed by the user with the public cloud before uploading this file.



Encrypt(PK,M,A). The encryption algorithm takes as input the public parameters PK, a message M, and an access structure A over the universe of attributes. The algorithm will encrypt M and produce a ciphertext CT such that only a user that possesses a set of attributes that satisfies the access structure will be able to decrypt the message. We will assume that the ciphertext implicitly contains A.

The decisional q-parallel Bilinear Diffie-Hellman Exponent problem as follows. Choose a group G of prime order p according to the security parameter. Let $a,s,b1,...,bq \in Zp$ be chosen at random and g be a generator of G. If an adversary is given

$Y= g,gs,ga,...,g(aq), ,g(aq+2),...,g(a2q)$

$\forall 1\leq j\leq q\ gs\cdot bj, ga/bj,...,g(aq/bj),,g(aq+2/bj),...,g(a2q/bj)$

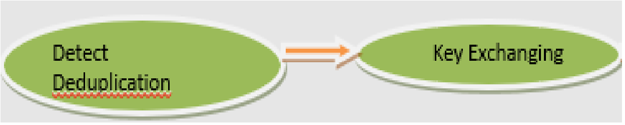
$\forall 1\leq j,k\leq q,k6=j\ ga\cdot s\cdot bk/bj,...,g(aq\cdot s\cdot bk/bj)$

4.3 Detect Deduplication

Convergent encryption provides data confidentiality in deduplication. A user derives a convergent key from each original data copy and encrypts the data copy with the convergent key.In addition, the user also derives a tag for the data copy, such that the tag will be used to detect duplicates.To detect duplicates, the user first sends the tag to the server side to check if the identical copy has been already stored**.**

4.4 Key Exchanging

The private keys for the privileges are managed by the private cloud the file token requests from the users.The interface offered by the private cloud allows user to submit files. In queries to be securely stored and computed respectively.The private cloud server will also check the user's identity before issuing the corresponding file token to the user. The authorized duplicate check for this file can be performed by the user with the public cloud before uploading this file.

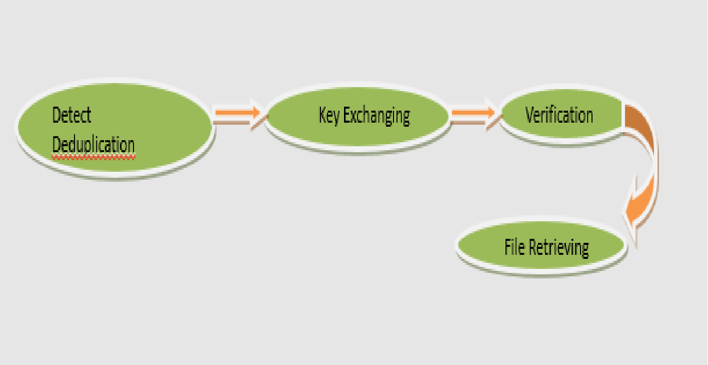


The mathematical expression is defined as,

$PrhB \sim y,T = e(g,g)aq+1s) = 0i - PrB \sim y,T = R= 0.$

4.5 Verification and File Retrieving

The private cloud server will also check the user's identity before issuing the corresponding file token to the user. An identification protocol use the proof and verification algorithm B Nrespectively. It also initializes a PoW protocol POW for the file ownership proof. In file retrieving it first sends a request and the file name to the S-CSP.Upon receiving the request and file name, the S-CSPwill check whether the user is eligible to download file.



Decrypt(PK,CT,SK): The decryption algorithm takes as input the public parameters PK, a ciphertext CT, which contains an access policy A, and a private key SK, which is a private key for a set S of attributes. If the set S of attributes satisfies the access structure A then the algorithm will decrypt the ciphertext and return a message M.

IV. CONCLUSION

Attribute-based encryption (ABE) has been widely used in cloud computing where data providers outsource their encrypted data to the cloud and can share the data with users possessing specified credentials. On the other hand, deduplication is an important technique to save the storage space and network bandwidth, which eliminates duplicate copies of identical data. However, the standard ABE systems do not support secure deduplication, which makes them costly to be applied in some commercial storage services. In this paper, we presented a novel approach to realize an attribute-based storage system supporting secure deduplication. Our storage system is built under a hybrid cloud architecture, where a private cloud manipulates the computation and a public cloud manages the storage. Though the above solution supports the differential privilege duplicate, it is inherently subject to brute force attacks launched by the public cloud server, which can recover files falling.The main idea of our technique is that the novel encryption key generation algorithm. For simplicity, we will use the hash functions to define the tag generation functions and convergent keys in this section.

REFERENCES

1. ”Attribute-Based Storage Supporting Secure Deduplication of Encrypted Data in Cloud “Hui Cui, Robert H. Deng, Yingjiu Li, and Guowei Wu, IEE TRANSACTION ON BIGDATA, VOL: PP, NO: 99, JAN 2017.
2. M. Bellare, S. Keelveedhi, and T. Ristenpart, “Message-locked encryption and secure deduplication,” in Advances in Cryptology- EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece,May 26-30, 2013. Proceedings, ser. Lecture Notes in ComputerScience, vol. 7881. Springer,2013, pp. 296–312.
3. M. Bellare and S. Keelveedhi, “Interactive message-locked encryption and secure deduplication,” in Public-Key Cryptography - PKC2015 - 18th IACR International Conference on Practice and Theory in Public-Key Cryptography, Gaithersburg, MD, USA, March 30 - April1, 2015, Proceedings, ser. Lecture Notes in Computer Science, vol.9020. Springer, 2015, pp. 516–538.
4. Y. Rouselakis and B. Waters, “Practical constructions and new proof methods for large universe attribute-based encryption,” in2013 ACM SIGSAC Conference on Computer and Communications Security, CCS’13, Berlin, Germany, November 4-8, 2013. ACM, 2013,
pp. 463–474.
5. P. Puzio, R. Molva, M. Onen, and S. Loureiro, “Cloudedup: Secure ̈deduplication with encrypted data for cloud storage,” in IEEE 5thInternational Conference on Cloud Computing Technology and Science, CloudCom 2013, Bristol, United Kingdom, December 2-5, 2013, Volume IEEE Computer Society, 2013, pp. 363–370.
6.]K. R. Choo, M. Herman, M. Iorga, and B. Martini, “Cloud forensics: State-of-the-art and future directions,” Digital Investigation, vol. 18, pp. 77–78, 2016.
7. Y. Yang, H. Zhu, H. Lu, J. Weng, Y. Zhang, and K. R. Choo, “Cloud based data sharing with fine-grained proxy re-encryption,” Pervasive and Mobile Computing, vol. 28, pp. 122–134, 2016.

Location Intimation and Video Monitoring System for School Children Using Raspberry Pi3 Based on IOT

Ms.S. Syedali Fathima,
UG Student
Department of Computer Science and Engineering,
Annai Teresa College of Engineering.

Mrs.A.Ramya,
Assistant Professor
Department of Computer Science and Engineering,
Annai Teresa College of Engineering.

Abstract –Security system and navigators have always been a necessity of human's life. Millions of children Millions of children need to travel between homes to school every day. Safer transportation of school children has been a critical issue as it is often observed that, kids find themselves locked in the school bus after going to school, they miss the bus, or ride. This project intends to find yet another solution to solve this problem by developing a bus safety system that will control the entry and exit of students from the buses through an efficient methodology. Due to the raise in number of kidnaps and road accidents, it is essential for the parents and school authorities to take necessary safety measures to avoid these plausible mishaps. Each child is provided with a Tag for the daily bus transportation to tag on a RFID reader present in the bus. It reads the tag value and sends the information to RPi3, which is then redirected to the GPS module; it can identify the location of the bus and send the information to parent's mobile through GSM providing the location of their child accordingly.

Index Terms - GSM, GPS, IOT, RFID module, raspberry pi3, live video streaming.

I. INTRODUCTION

The concept is based on RFID system. This system is used to track the attendance of the students in the school bus. In today's generation children lack in skill to protect themselves, so it is our responsibility as a person to safe guard children and to teach them the skills to be safe. Today most of the students are travelling to school buses or vans. Parents think that their kids are safe when they travel by school bus. But are they really safe there are many common problems such as students getting kidnapped out of school, bus getting delayed in traffic etc. sowe can't exactly say that they are safe with bus. So now it's possible to track the bus, find out whether they are in trouble or why they are late by school bus tracking project. By enhancing this project we can make additional services to the society like daily traffic analysis the bus can send through the most suitable route which will help to reduce traffic in urban area. Many unpleasant incidents relating to school buses have taken place questioning the safety of children using that services. So, it‘s become vital for the parents to monitor their children throughout their travel. In this paper, we focus on a particular risk associated with the daily bus trip to and from school. There have been previous incidents where a child is forgotten in the bus and eventually die because of suffocation. In this paper, the design of an efficient system is presented, which allows parents to watch over their children, their bus journey directly by providing them with location and continuous live video streaming. The location of the bus at that current moment is identified by the GPS, and a message is returned to the parent‘s mobile providing the same along with date and time. The proposed system also provides a live video streaming option to the parents, using a sanctioned IP address which also provides the student‘s detail database making easy even for the school administration to monitor the location of buses and children travelling in them.

II. RELATED WORKS

Range and Obstacle detection and accident detected sensors are implanted on the front surface of the bus in order to avoid collision with another vehicle on the Road. Each student is tagged with unique code. Two counters used at the entrance and exit location of the bus. Wireless communication technology (IEEE 802.4.15) is used to inform the status of the bus to the school principal. To solve the problem by developing a bus safety system that will control the entry and exit of students from the buses through an energy efficient methodology. This system will control the entry and exit of students to and from the bus using RFID (Radio Frequency Identification) and GSM technologies to ensure the entering and exiting of all students to and from the school bus in a safely manner. To communicate between the server and the user present at the remote location, various systems can be used such as zigbee, Bluetooth, etc. But among all of them, GSM system is found to be most useful due to its range and efficiency as nowadays everyone is having a cell phone. Here the GSM-GPS technology is to track the children students. GPS is used for identifying the student location. GSM is used to send the information to the parent android mobile. Monitoring database is provided at the control room of the school.

III. PRPOSED SYSTEM

The proposed system is shown in Figure 1. This system uses Raspberry Pi3 as the chief module. RFID Tags are worn by the each student by which every parent can track their respective kid‘s current location. RFID reader used reads the Tag‘s value which is a 12 digit code and sends the results to RPi3 Module. GPS provides reliable positioning and timing of the children. GSM sends the information to parents accordingly. USB web camera provides live stream of students inside the bus; this video monitoring and student‘s data information is provided to parents and school administration via IP address. The proposed system is implemented using a Raspberry Pi 3 Model B. Raspberry pi is a mini computer. It is a Credit – Card Sized Computer Manufactured and Designed in the UK by the Raspberry Pi Foundation.

Interconnections and interfacings for this system, this Paper every student has unique tag that contains 12 digit code specifying the child‘s identity. This Child tag tags on the RFID reader, it reads the tag value and sends the information to RPi3, which is then redirected to the GPS module; it can identify the location of the bus and send the information to parent‘s mobile through GSM providing the location of their child accordingly. At any moment, if parents want to know their kid‘s location, they can simply send a request message as Where‖ to the authorized phone number on the bus. The location of the bus at that current moment is identified by the GPS, and a message is returned to the parent‘s mobile providing the same along with date and time. The proposed system also provides a live video streaming option to the parents, using a sanctioned IP address which also provides the student‘s detail database making easy even for the school administration to monitor the location of buses and children travelling in them.

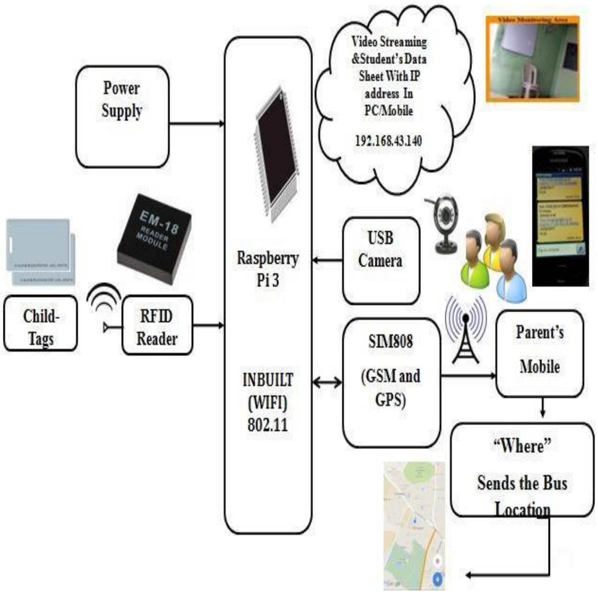


Figure 3.1- Architecture of the system

3.1 Raspberry Pi3

Raspberry pi3 is a Credit – Card Sized Computer Manufactured and Designed in the UK by the Raspberry Pi Foundation. It is capable of several things such as, spreadsheets, word-processing and high-definition videos and games. It has a Broadcom BCM2837, an ARM Cortex-A53 64bit Quad Core Processor System-on-Chip and Linux-based operating system. It can do multi functionalities at a time.

Figure 3.2 - Raspberry pi3

3.2 RFID Readers And RFID Tags

Radio **F**requency **I**dentification is a technology that can use radio-frequency waves to transfer data between reader and a movable item to identify or track etc. Generally a RFID system consists of 3 arts those are: Readers, Antennas and Tags (transponders).

3.3 GSM Module

The SIM 900 is a compatible Quad - band cell phone, which works on a frequency 850/900/1800/1900 MHZ and which can be used not only to access the internet, but also for oral communication (provided that it is connected to a microphone and a small loud speaker) and for SMS. GSM solution in a SMT module which can be embedded in the application. It is an ultra-compact and reliable wireless module.

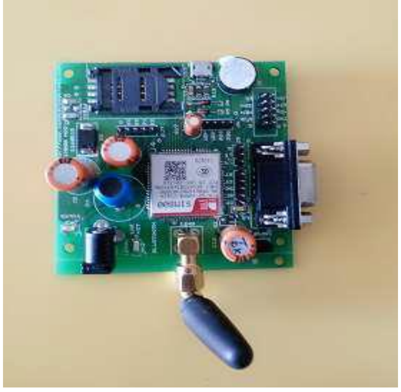


Figure 3.3 - GSM Module

The Raspberry Pi board is interfaced with all modules; it is driven by 230V AC power supply, transferred through step-down transformer and reduced to 12V AC power further transferred through bridge rectifier and converted to 12V DC power supply. Filter capacitors are used for smoothing the waveform received from the rectifier. A Voltage regulator is a device which converts varying input voltage into a constant regulated output voltage of 5V DC. This 5V is given to all modules of this system. After first process, child tag can tag on the RFID reader; it can access the tag value and then that reading can be sent to RPi3 module. It can verify the child tag which is accessed by reader to check the child who got into or got down the bus, based on the counting of the reader and get the position of the child is received by GPS receiver from SIM808 module. This result can be sent to parent‘s mobile through GSM. Whenever child gets into the bus parents get a message it shows," Your child started to school" vehicle position with longitude and latitude values. Whenever child gets down the bus parents get message "Your child started to house" vehicle position with longitude and latitude values. SMS when Child got down the bus At any moment, if parents want to know their kid‘s location, they can simply send a request message as "Where" to the authorized phone number on the bus. The location of the bus at that current moment is identified by the GPS, and a message is returned to the parent‘s mobile providing the same along with date and time Parents can view child‘s current position by clicking the link received in the message in Google maps shown in fig 3.4.

Figure 3.4 - Location identifying

3.4 Live Video Streaming

This system can also provide the information of the child‘s location through continuous live streaming and student‘s data information can be is provided in this system The entire system interfacings with all the modules connecting to RPi3. Power supply is given by the micro USB power input; upgraded switched power source that can handle up to 2.5 Amps. RPi3 40(GPIO 21) used for LED activation. GPIO 6 and 9 Pins are used for ground. USB1 can be connected to USB camera for the video monitoring of the student in the school bus.USB2 can be connected to SIM 808 Module which consists of GPS receiver and GSM Module together. USB3 can be used for receiving data from RFID reader. USB2 and USB3 are connected in TTL to serial converter can be used for Transmitting and Receiving of the data.

3.5 Internet Of Things

The Internet of things (IoT) is the network of physical devices, vehicles, home appliances andotheritems embedded with electronics, software, sensors, actuators,and connectivity whic h enables these objects to connect and exchange data. Each thing is uniquely identifiable through its embedded computing system but is able to inter-operate within the existing Internet infrastructure. This system uses IOT for communication between the user and the server.

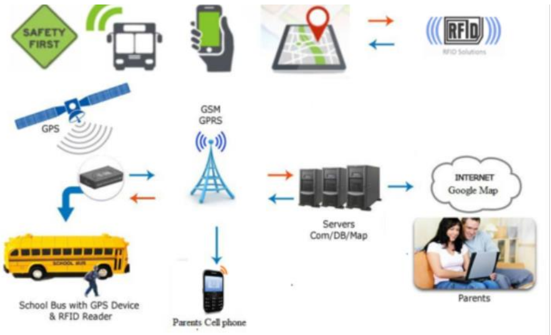


Figure 3.5 -IOT based system

IV. CONCLUSION

This system focuses on monitoring child's position and sends it to their parents respectively; it also responds to parent's requests, providing their child's current location. Parents can access student's data information and live monitoring continuously using a web page based on IOT with an IP address. Implementation cost is reasonable, Smart and user friendly. The security level can be extended at any place in the school, e.g. Libraries, and Classrooms. This can be made even more secure using Biometric measures, which can be used at any Educational Institutions. These technologies may also implement in Android for managing records, location identifying, live stream video etc. Application offers reliability, time consuming and easy control.

REFERENCES

1. Bichlin Hoang and Ashley Caudill "IEEE Emerging Technology." 2006-2012.
2. Asaad M. J. "Experimentally Evaluations of GPS Based system design." 19th March 2012.
3. Bruno Crispo, Melanie R. Rieback, Andrew S. Tanenbaum "The Evolution of RFID security" International 4 year old, forgotten in a school bus, dies‖. Available at:http://www.muscatdaily.com/Archive/Oman/4-year-old-forgotten-in-a-school-bus-dies [Accessed: 11 Aug. 2014] .
4. Toumi, H., ―Four-year-old girl left alone in school bus dies‖. Available at: http://gulfnews.com/news/gulf/qatar/four-year-old-girl-left-alone-in-school-bus-dies-1.628394 [Accessed: 11 Aug. 2014] .
5. K.VidyasagarG.BalajiK.NarendraReddy Dept. of ECE, SSIT Sathupally, T.S, India "RFID-GSM Imparted School Children Security System" Communications on

Applied Electronics (CAE) – ISSN : 2394-4714 Foundation of Computer Science FCS, New York, USA Volume 2 – No.2, June 2015.

6. Anwar Ali-Lawati, Shaikha Al-Jahdhami, Asma Al-Belushi, Dalal Al-Adawi,MedhatAwadalla and Dawood Al-Abri, Department of Electrical and Computer Engineering, Sultan Qaboos University, ―RFID Based System for school children transportation safety enhancement‖ proceedings of the 8th IEEE gcc conference and exhibition,muscat,oman.1- 4 february,2015.
7. M.Navya,― android based children tracking system using voice recognition‖, International journal of Computer science and information technology, Vol 4 (1): pages 229-235, Jan 2015.
8. ”The Official Raspberry Pi projects book” Available at: https://www.raspberrypi.org/magpi-issues/Projects_Book_v1.pdf

Secure and Trusted Information Brokering in Cloud Computing

Ms. T.Hemalatha,
Assistant Professor,
Department of Computer Science and Engineering,
Krishnasamy College of Engineering and Technology

Mr. D.Vignesh, Mr. P.Punidhan,
UG Students,
Department of Computer Science and Engineering,
Krishnasamy College of Engineering and Technology

Abstract - To facilitate extensive collaborations, today's organizations raise increasing needs for information sharing via on- demand information access. Information Brokering System (IBS) a top a peer-to-peer overlay has been proposed to support information sharing among loosely federated data sources. In this article, we study the problem of privacy protection in information brokering process. We first give a formal presentation of the threat models with a focus on two attacks: attribute-correlation attack and inference attack. Then, we propose a broker-coordinator overlay, as well as two schemes, automaton segmentation scheme and query segment encryption scheme, to share the secure query routing function among a set of brokering servers. With comprehensive analysis on privacy, end to- end performance, and scalability, we show that the proposed system can integrate security enforcement and query routing while preserving system-wide privacy with reasonable overhead. Finally, T-broker uses a lightweight feedback mechanism, which can effectively reduce networking show that, compared with the existing approaches, our T-broker yields very good results in many typical cases, and the proposed system is robust to deal with various numbers of dynamic service behavior from multiple cloud sites risk and improve system efficiency.

Index Terms - ***Information Broking System, Automation segmentation, coordinates broker, privacy preserving, and Attribute-correlation attack***

I. INTRODUCTION

In recent years, we have observed an explosion of information shared among organizations in many realms ranging from business to government agencies. To facilitate efficient large-scale information sharing, many efforts have been devoted to reconcile data heterogeneity and provide interoperability across geographically distributed data sources.

In the context of sensitive data and autonomous data owners, a more practical and adaptable solution is to construct a data centric overlay including the data sources and a set of brokers helping to locate data sources for queries Such infrastructure builds up semantic-

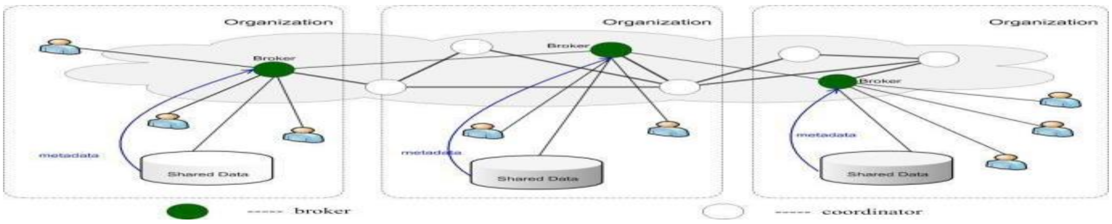


Figure 1: An overview of the IBS infrastructure

aware index mechanisms to route the queries based on their content, which allows users to submit queries without knowing data or server location.

.To prevent curious or corrupted coordinators from inferring private information, we design two novel schemes: (a) to segment the query brokering automata, and (b) to encrypt corresponding query segments. While providing full capability to enforce in-network access control and to route queries to the right data sources, these two schemes ensure that a curious or corrupted coordinator is not capable to collect enough information to infer privacy, such as "which data is being queried", "where certain data is located", or "what are the access control policies", etc. We show that PPIB provides comprehensive privacy protection for on-demand information brokering, with insignificant overhead and very good scalability.

II. RELATED WORK

Research areas such as information integration, peer-to- peer file sharing systems and publish-subscribe systems provide partial solutions to the problem of large scale data sharing. Information integration approaches focus on providing an integrated view over large numbers of heterogeneous data sources by exploiting the semantic relationship between schemas of different sources.

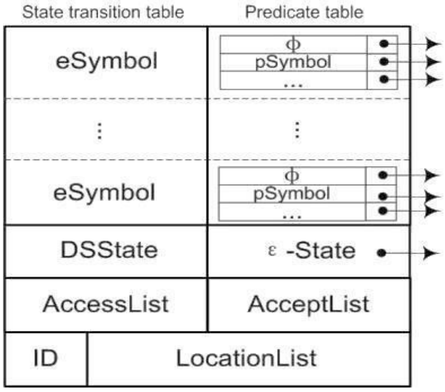


Figure 2 : Data structure of an NFA state.

2.1 Vulnerabilities and The Threat Model

In a typical information brokering scenario, there are three types of stakeholders, namely data owners, data providers, and data requestors. Each stakeholder has its own privacy:

(1) The privacy of a data owner (e.g. a patient in RHIO) is identifiable data and the information carried by this data (e.g. medical records). Data owners usually sign strict privacy agreements with data providers to protect their privacy from unauthorized disclosure/use.

(2) Data providers store collected data, and create two types of metadata, namely routing metadata and access control metadata, for data brokering. Both types of metadata are considered privacy of a data provider.

(3) Data requestors disclose identifiable and private information in the querying process.

For example, a query about AIDS treatment reveals the (possible) disease of the requestor.

2.2 Attribute Correlation Attack

An attacker intercepts a query (in plaintext), which typically contains several predicates. Each predicate describes a condition, which sometimes involves sensitive and private data (e.g. name, SSN or credit card number, etc.). If a query has multiple predicates or composite predicate expressions, the attacker can "correlate" the corresponding attributes to infer sensitive information about the data owner. This attack is known as the attribute correlation attack:

III. EXISTING SYSTEM

3.1 Privacy-Preserving Query Brokering Scheme

While QBroker seamlessly integrates the content-based indexing function into the NFA-based access control mechanism, it heavily relies on the QBroker for the enforcement and shifts all the data (i.e., the ACR, index rules, and user queries) to it. However, if the QBroker is compromised or no longer assumed fully trusted (e.g. under the honest-but-curious assumption as in our study), the privacy of both the requestor and the data owner is under risk.

3.2 Automaton Segmentation

In the context of distributed information brokering, multiple organizations join a consortium and agree to share the data within the consortium. While different organizations may have different schemas, we assume a global schema exists by aligning and merging the local schemas. Thus, the access control rules and index rules for all the organizations can be crafted following the same shared schema and captured by a global automaton, the global QBroker. The key idea of the automaton segmentation scheme is to logically divide the global automaton into multiple independent yet connected segments, and physically distribute the segments onto different brokering servers.

Segmentation: The atomic unit in the segmentation is an NFA state of the original automaton. Each segment is allowed to hold one or several NFA states. We further define the granularity level to denote the greatest distance between any two NFA states contained in one segment. Given a granularity level k, for each segmentation, the next i 2 [1; k] NFA states will be divided into one segment with a probability 1=k. As privacy protection is of the primary concern of this work, we suggest a granularity level

1) To reserve the logical connection between the segments after segmentation, we define heuristic segmentation rules:
2) Multiple NFA states in the same segment should be connected via parent-child links;
3) No sibling NFA states should not be put in the same segment without the parent state; and
4) The "accept state" of the original global automaton should be put in separate segments. To ensure the segments are logically connected,
5) We change the last states of each segment to be "dummy" accept states, which point to the segments holding the child states in the original global automaton.

IV. SYSTEM IMPLEMENTATION

As mentioned above, most current cloud brokering systems do not provide trust management capabilities to make trust decisions, which will greatly hinder the development of cloud computing. depicts the brokering scenario in existing and Aeolus We can see that this existing brokering architecture for cloud computing do not consider user feedback only relying on some direct monitoring information. Before introducing the principles for assessing, representing and computing trust, we first present the basic architecture of T-broker and a brief description of its internal components.

4.1 Sensor-Based Service Monitoring (SSM)

This module is used to monitor the real-time service data of allocated resources in order to guarantee the SLA (Service Level Agreement) with the users. In the interactive process, this module dynamically monitors the service parameters and is responsible for getting run-time service data. The monitored data is stored in the evidence base, which is maintained by the broker.

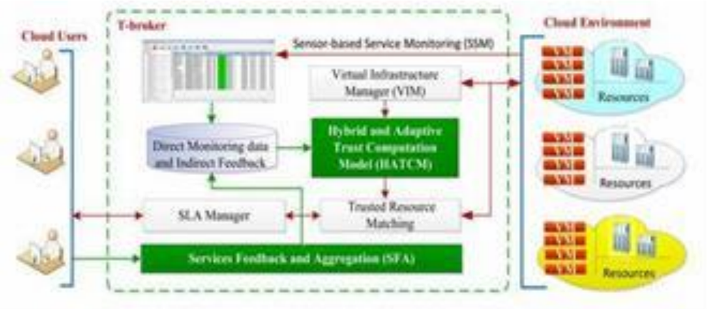

Cloud Users
T-broker
Sensor-based Service Monitoring (SSM)
Cloud Environment
Virtual Infrastructure Manager (VIM)
Direct Monitoring data and Indirect Feedback
Hybrid and Adaptive Trust Computation Model (HATCM)
SLA Manager
Trusted Resource Matching
Services Feedback and Aggregation (SFA)
VM
Resources
Resources
Resources

Figure 4 : Proposed Architecture

The node spec profile includes four trusted evidences: CPU frequency, memory size, hard disk capacity and network bandwidth. The average resource usage information consists of the current CPU utilization rate, current memory utilization rate, current hard disk utilization rate and current bandwidth utilization rate. The number of malicious access includes the number of illegal connections and the times of scanning sensitive ports.

V. PROPOSED SYSTEM

The proposed system is robust to deal with various numbers of dynamic service behavior from multiple cloud sites. Some hybrid trust models are proposed for cloud computing environment It is no doubt that how to adaptively fuse direct trust (first-hand trust) and indirect trust (users feedback) should be an important problem, however, most current studies in hybrid trust models either ignore the problem or using subjective or manual methods to assign weight to this two trust factors. The proposed trust management framework for a multi- cloud environment is based on the proposed trust evaluation model and the trust propagation network. First, a trusted third party-based service brokering architecture is proposed for multiple cloud environments, in which the T-broker acts as a middleware for cloud trust management and service matching. T-broker uses a hybrid and adaptive trust model to compute the overall trust degree of service resources, in which trust is defined as a fusion evaluation result from adaptively combining the direct monitored evidence with the social feedback of the service resources.

5.1 Trust-aware brokering architecture

In which the broker itself acts as the TTP for trust management and resource scheduling. Through distributed soft-sensors, this brokering architecture can real-time monitor both dynamic service behavior of resource providers and feedbacks from users.

5.2 Hybrid and Adaptive Trust Computation Model (HATCM)

A hybrid and adaptive trust model to compute the overall trust degree of service resources, in which trust is defined as a fusion evaluation result from adaptively combining dynamic service behavior with the social feedback of the service resources. The HATCM allows cloud users to specify their requirements and opinions when accessing the trust score of cloud providers. That is, users can specify their own preferences, according to their business policy and requirements, to get a customized trust value of the cloud providers

5.3 Maximizing deviation method (MDM)

A maximizing deviation method to compute the direct trust of service resource, which can overcome the limitations of traditional trust models, in which the trusted attributes are weighted manually or subjectively. At the same time, this method has a faster convergence than other existing approaches.

5.4 Sensor-Based Service Monitoring (SSM)

This module is used to monitor the real-time service data of allocated resources in+ order to guarantee the SLA (Service Level Agreement) with the users. In the interactive process, this module dynamically monitors the service parameters and is responsible for getting run- time service data. The monitored data is stored in the evidence base, which is maintained by the broker. To calculating QoS-based trustworthiness of a resource we mainly focus on five kinds of trusted attributes of cloud services, which consists of node spec profile, average resource usage information, average response time, average task success ratio, and the number of malicious access.

5.5 Virtual Infrastructure Manager (VIM)

Each cloud provider offers several VM configurations, often referred to as instance types. An instance type is defined in terms of hardware metrics such as CPU frequency, memory size, hard disk capacity, etc. In this work, the VIM component is based on the Open Nebula virtual infrastructure manager this module is used to collect and index all these resources information from multiple cloud providers.

5.6 Service level agreement Manager (SLA)

In the multiple cloud computing environment, SLA can offer an appropriate guarantee for the service of quality of resource providers, and it serves as the foundation for the expected level of service between the users and the providers An SLA is a contract agreed between a user and a provider which defines a series of service quality characters. Adding trust mechanism into the SLA management cloud brokering system can prepare the best trustworthiness resources for each service request in advance, and allocate the best resources to users.

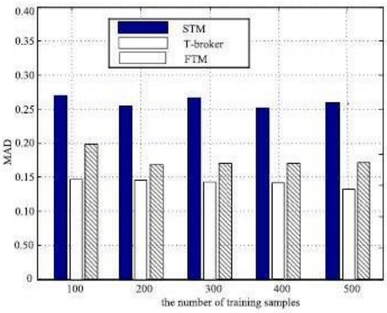
5.7 Multiple Clouds Computing

MULTIPLE cloud theories and technologies are the hot directions in the cloud computing industry, which a lot of companies and government are putting much concern to make sure that they have benefited from this new innovation .

5.8 Accuracy Evaluation

The value of εri (λ) is used to measure the degree of deviation of calculating results; thus, the closer its value is to zero, the higher the calculating accuracy. First, observing MAD under conditions with different number of training samples(Note: we gather a training sample dt= (dt1, dt2, . . . , dtm) at each time-stamp t, so the number of training samples equals to the number of time-stamps). In order to observe experimental results under different scale of training samples, we use two kinds of inputting samples, a small number of training samples and a large number of training samples.

Figure 5: The values of MAD with a large number of training samples.



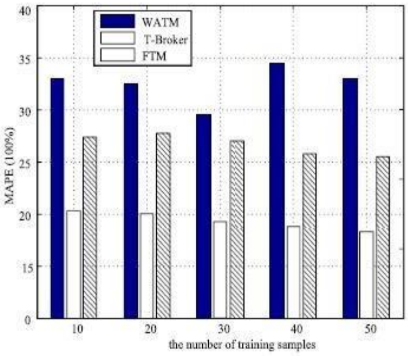


Figure 6 : The values of MAPE with a small number of training samples.

The MAPE is a measure of accuracy in a fitted time series value in statistics, specifically trending. It usually expresses accuracy as a percentage. MAPE can reflect the unbiasedness of the calculating model. A smaller value of MAPE reflects the calculating model has better and unbiased accuracy. We also use two kinds of inputting samples to evaluate the MAPE of the three models, a small number of training samples and a large number of training samples.

VI. CONCLUSION

In this paper, we present T-broker, a trust-aware service brokering system for efficient matching multiple cloud services to satisfy various user requests. Experimental results show that T-broker yields very good results in many typical cases, and the proposed mechanism is robust to deal with various number of service resources. In the future, we will continue our research from two aspects. First is how to accurately calculate the trust value of resources with only few monitored evidences reports and how to motivate more users to submit their feedback to the trust measurement engine. Implementing and evaluating the proposed mechanism in a large-scale multiple cloud system, such as distributed data sharing and remote computing, is another important direction for future research.

REFERENCES

1. Hamid Sadeghi (2011), "Empirical Challenges and solutions in constructing a high-performance metasearch engine", emeraldinsight.
2. C.Swaraj Paul , G. Gunasekaran, "A Descriptive Literature Survey on Search of Data inCloud " in International Journal of Applied Engineering Research IJAER, pp. 13112-13114, Volume 10, Number 17 (2015) Special Issues, ISSN 0973- 4562.

Anatomical Functional Image Fusion by Using Local Laplicial Filtering Techniques.

Mr. Chandru.V, Mr. Sivabalan.J,
UG Students,
Department of Computer Science and Engineering,
Annai Teresa College of Engineering

Mr.A.Arivazhagan,
Assistant Professor,
Department of Computer Science and Engineering,
Annai Teresa College of Engineering

Abstract* – A novel method for performing anatomical magnetic resonance imaging-functional (positron emission tomography or single photon emission computed tomography) image fusion is presented. The method merges specific feature information from input image signals of a single or multiple medical imaging modalities into a single fused image, while preserving more information and generating less distortion. The proposed method uses a local Laplacian filtering-based technique realized through a novel multi-scale system architecture. First, the input images are generated in a multi-scale image representation and are processed using local Laplacian filtering. Second, at each scale, the decomposed images are combined to produce fused approximate images using a local energy maximum scheme and produce the fused residual images using an information of interest-based scheme. Finally, a fused image is obtained using a reconstruction process that is analogous to that of conventional Laplacian pyramid transform. Experimental results computed using individual multi scale analysis-based decomposition schemes or fusion rules clearly demonstrate the superiority of the proposed method through subjective observation as well as objective metrics. Furthermore, the proposed method can obtain better performance, compared with the state-of-the-art fusion methods.

Index Terms—**Image fusion, multi-scale decomposition, interest-based rule**.

I. INTRODUCTION

Medical imaging data allows for increased performance in a wide range of clinical applicability of medical images for diagnosis and assessment of medical problems. Over the past decades, anatomical-functional fusion systems such as MRI-PET and MRI-SPECT have been seen as a new hybrid molecular imaging technology. MRI image provides anatomical contrast of soft-tissue structure at a high spatial resolution. However, it lacks activity. information about soft tissues. In contrast, PET images provide high contrast for accurately tracing tumors. SPECT imaging is used to study blood flow in tissues and organs using nuclear imaging techniques. However, PET and SPECT images have low resolution. The goal of an MRI-PET or MRI-SPECT system is to merge multiple images from a single or from multiple imaging modalities into a fused image while preserving specific feature information. The benefits of an MRI-PET or MRI-SPECT system can be achieved by simple image fusion for some basic clinical brain examinations because the skull provides a frame of reference for the soft tissue of the brain [4]–[6]. In this paper, we focus on image fusion methods for MRI-PET or MRI-SPECT systems in the clinical study of brain tumors.

Due to the advantages of low computational complexity and simple implementation, a large number of research papers have focused on pixel-level fusion methods. Therefore, an image fusion method at the pixel level is presented in this paper. Multi-modal pixel-level medical image fusion has attracted a considerable amount of attention in recent years. Multiscale analysis (MSA) tools have achieved the best fusion performance. In contrast to single-scale based fusion methods, MSA-based fusion methods have the advantage of extracting and combining much more image feature information at different scales. MSA-based fusion methods can be summarized by the following steps: image decomposition, image fusion rule construction and adoption, and image reconstruction. Image decomposition is performed first by transforming the input images into their multi-scale image representations. The process separates the image signals into sub-band images at high-frequency and low-frequency resolutions. The high-frequency images contain more detailed information from the original images, while the low- frequency images provide coarser image features. The fusion scheme then creates new image fusion rules for combining the high frequency images and low-frequency images. After obtaining the fused high-frequency images and the fused low- frequency images, the inverse image decomposition transform is used to reconstruct the output fused image. Traditionally, image decomposition in MSA can be divided into two categories: the pyramid transform and the parallelepiped transform In the first class of fusion methods such as the Laplacian pyramid transform (LAP) ,gradient pyramid transform (GRP), curvelet transform (CVT),contourlet transform (COT) [13] and shearlet transform (ST) , each level of the sub-band image results from subsampling the corresponding level. The subsampled sub-band at each level is the result of the successive reduction by a factor of 2 of the image resolution in the pyramid transform domain.

However, these kinds of methods may produce some distortion in the resulting image, which appears obvious when considering the subsampling algorithm. The second class of fusion methods was proposed to fuse multiple images using a non sub sampling process in a multi-scale scheme. In the parallelepiped scheme, all approximated images have the same number of columns and rows as the input images using the image filter filled with zeroes. When climbing up through the resolution levels, the successive approximation images have a coarser resolution while remaining the same size as the input images. Parallelepiped-based fusion methods, such as the non sub sampled contourlet transform (NSCT), the support value transform (SVT) , and the neighborhood distance transform (ND), have been recognized as efficient shift invariant image representations. NSCT was developed from the non sub sampled LAP and the non sub sampled directional filter bank. In addition, SVT is constructed by combining non sub sampled LAP and a support value filter.

In PCA, the fused image is a combination of the principal components of the inputs. In particular, PCNN and SR methods usually include two stages: training and testing .In the first stage, a large number of images are used in training to achieve optimal image pixel values. In the second stage, the fused image is obtained by implementing arithmetic operators on the trained optimal image pixel values. However, PCNN and SR methods take a long time because of the training stage. To incorporate spatial information, the DSIFT and SUSAN descriptors are adopted to detect points of interest, with the purpose of preserving prominent texture and edge information in the input Image.

In the proposed method, local Laplacian filtering (LLF) is selected as the multi-scale imaged composition tool for processing the input MRI, PET, and SPECT images. It can be clearly observed that LAP is the basis of MSA tools, as mentioned above. However, traditional LAP is unable to represent edge information well. To overcome this limitation, LLF is used not only to preserve structural information but also to enhance detail information. Then, two image fusion rules are constructed for combining the
approximate and residual images.

II. RELATED WORK

Multiscale contrast enhancement for radiographies: Laplacian pyramid versus fast wavelet transform.Contrast enhancement of radiographies based on a multiscale decomposition of the images recently has proven to be a far more versatile and efficient method than regular unsharp-masking techniques, while containing these as a subset. In this paper, we compare the performance of two multiscale methods, namely the Laplacian Pyramid and the fast wavelet transform (FWT). We find that enhancement based on the FWT suffers from one serious drawback-the introduction of visible artifacts when large structures are enhanced strongly. By contrast, the Laplacian Pyramid allows a smooth enhancement of large structures, such that visible artifacts can be avoided. Only for the enhancement of very small details, for denoising applications or compression of images, the FWT may have some advantages over the Laplacian Pyramid.

A method to reduce the Gibbs ringing artifact in MRI scans while keeping tissue boundary integrity.Gibbs ringing is a well known artifact that effects reconstruction of images having discontinuities. This is a problem in the reconstruction of magnetic resonance imaging (MRI) data due to the many different tissues normally present in each scan. The Gibbs ringing artifact manifests itself at the boundaries of the tissues, making it difficult to determine the structure of the brain tissue. The Gegenbauer reconstruction method has been shown to effectively eliminate the effects of Gibbs ringing in other applications. This paper presents the application of the Gegenbauer reconstruction method to neuro-imaging Orthogonal distance fitting of implicit curves and surfaces.

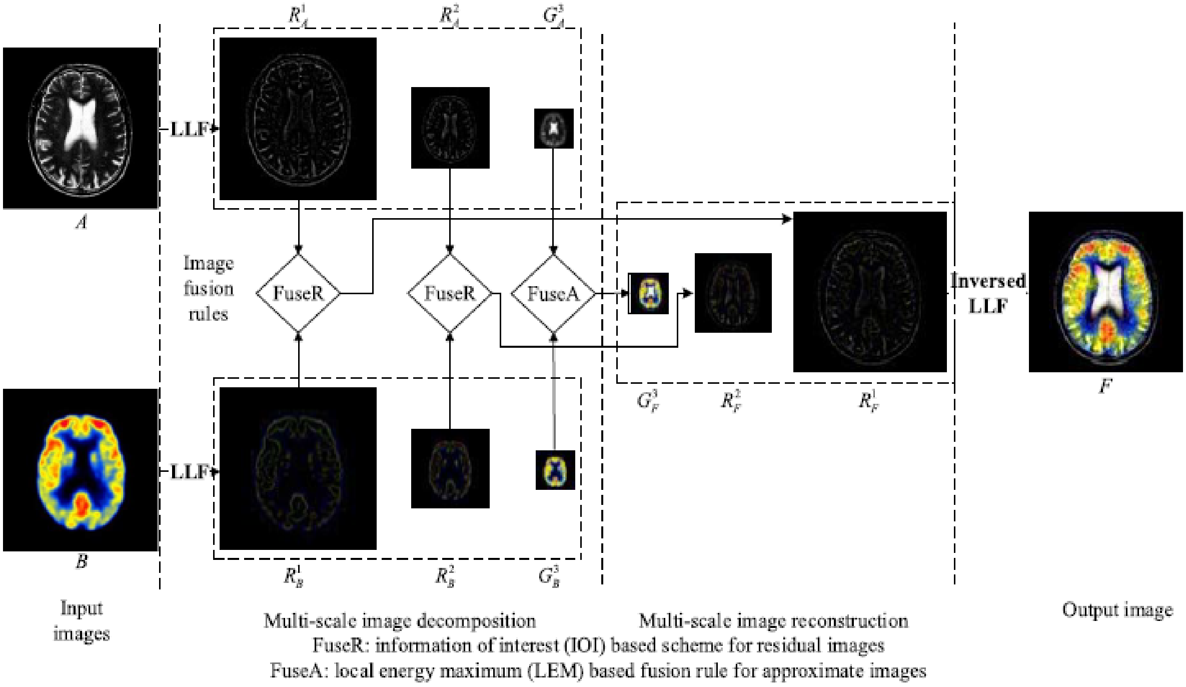
Computation and visualization of three-dimensional soft tissue motion in the orbit. Complex-bilinear recurrent neural network for equalization of a digital satellite channel. Classification of disease subgroup and correlation with disease severity using magnetic resonance imaging whole-brain histograms: application to magnetization transfer ratios and multip...Custom implant design for patients with cranial defects. Medical image reconstruction, processing, visualization, and analysis: the MIPG perspective. Encoding with frames in MRI and analysis of the signal-to-noise ratio.

III. LOCAL LAPLICIAN FILTERING

Edge-preserving filters enhance detail information in an image while preserving the sharpness of its edge information. Edge-preserving filters have wide applications in the fields of medical imaging, such as medical image restoration , medical image denoising , and

medical image fusion . In the field of medical image fusion, authors have constructed new multi-scale image decomposition and reconstruction schemes and new image fusion rules based on edge-preserving filters .The advantage of edge preserving filters in medical image fusion is that medical images can be fused and enhanced simultaneously. n the proposed method, LLF, an edge-preserving filter, is adopted as the multi-scale image decomposition and reconstruction tool. Compared with other edge-preserving filters, the advantages of LLF are that: LLF is based on the traditional standard Laplacian pyramid method. LLF operates on raw pixels rather than solving an optimization problem. LLF models edge information in an input image using a simple threshold of pixel values to differentiate large-scale edge information from small-scale detail information. LAP filtering has been applied to fuse medical images with different modalities at multiple scales. However, the fused image introduces degrading edges and halos. To overcome these limitations, LLF is proposed, given its advantages of simplicity and flexibility. Please refer to Table I for important definitions used throughout the rest of this paper. In theory, LLF assumes that the filtered output *O* is constructed by computing a new LAP for the intermediate image
coefficients *S _I __* at each scale *i* .

$$O = \text{collapse}(Si\ \_I\ \_\_).$$


R_A^1
R_A^2
G_A^3
LLF
A
Image fusion rules
FuseR
FuseR
FuseA
Inversed LLF
F
G_F^3
R_F^2
R_F^1
LLF
B
R_B^1
R_B^2
G_B^3
Input images
Multi-scale image decomposition
Multi-scale image reconstruction
Output image
FuseR: information of interest (IOI) based scheme for residual images
FuseA: local energy maximum (LEM) based fusion rule for approximate images

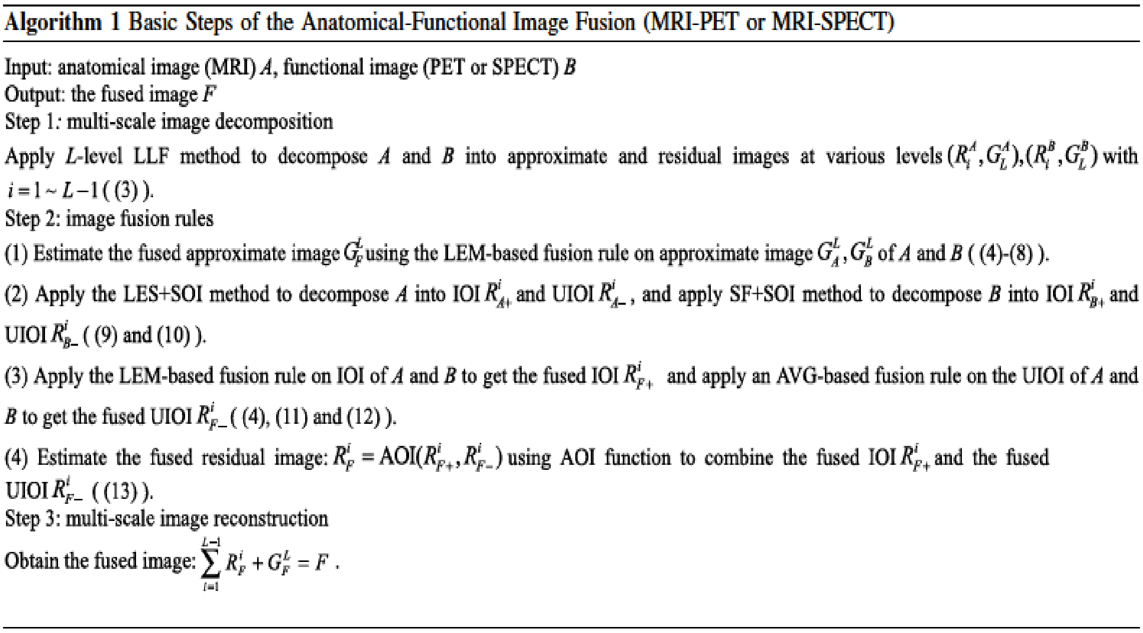
For each coefficient *v* = *(x, y, i)* in the image *I _*, we generate a new coefficient *I _(v)* by applying a point-wise remapping function,

$$I\ \_(v) = \{\ g + \text{sign}(v - g)(\beta(|v - g| - \sigma r) + \sigma r), \text{ otherwise},$$

$$g + \text{sign}(v - g)\sigma r(|v - g|/\sigma r)\alpha, \quad i\ f\ |v - g| \leq \sigma r$$

where *(x, y)* represents the pixel coordinate in horizontal orientation and vertical orientation, *i* represents the level of the pyramid, sign denotes signal function, *v* is the pixel value at the position *(x, y)*, and *g* is value of the image resulting from the Gaussian pyramid. Furthermore, in there are three free parameters in LLF: the intensity threshold *σr* , the detail parameter *α*, and the edge parameter *β*. The intensity threshold *σr* acts as the threshold for differentiating edge information from detail information. If $|v - g| \leq \sigma r$, *v* should be processed as detail information. Otherwise, *v* should be processed as edge information. The detail parameter *α* is closely related to detail information. The edge parameter *β* is closely related to edge information. If $0 < \alpha < 1$ and $\beta = 1$, LLF of the input image is a detail enhancement operation. If $\alpha = 1$ and $0 \leq \beta < 1$, LLF of the input image is edge-aware compression. If $\alpha = 1$ and $\beta = 1$, the input image coefficient is not changed. Moreover, for a color input image, the filtered output is obtained by applying LLF to the red, green, and blue (RGB) channels of the input image. In conclusion, when the edge parameter $\beta = 1$, LLF evolves into filtering of details.

In the proposed method, we want to preserve the edge sharpness and enhance detail information in the fused image. Therefore, the edge parameter *β* is set at 1. In addition, after many experiments, the intensity threshold *σr* was set at 0.4 and the detail parameter *α* was set at 0.25.



Algorithm 1 Basic Steps of the Anatomical-Functional Image Fusion (MRI-PET or MRI-SPECT)

```
Input: anatomical image (MRI) $A$, functional image (PET or SPECT) $B$
Output: the fused image $F$
Step 1: multi-scale image decomposition
Apply $L$-level LLF method to decompose $A$ and $B$ into approximate and residual images at various levels $(R_i^A, G_L^A), (R_i^B, G_L^B)$ with $i = 1 \sim L-1$ ( (3) ).
Step 2: image fusion rules
(1) Estimate the fused approximate image $G_F^L$ using the LEM-based fusion rule on approximate image $G_A^L, G_B^L$ of $A$ and $B$ ( (4)-(8) ).
(2) Apply the LES+SOI method to decompose $A$ into IOI $R_{A+}^i$ and UIOI $R_{A-}^i$ , and apply SF+SOI method to decompose $B$ into IOI $R_{B+}^i$ and UIOI $R_{B-}^i$ ( (9) and (10) ).
(3) Apply the LEM-based fusion rule on IOI of $A$ and $B$ to get the fused IOI $R_{F+}^i$ and apply an AVG-based fusion rule on the UIOI of $A$ and $B$ to get the fused UIOI $R_{F-}^i$ ( (4), (11) and (12) ).
(4) Estimate the fused residual image: $R_F^i = \mathrm{AOI}(R_{F+}^i, R_{F-}^i)$ using AOI function to combine the fused IOI $R_{F+}^i$ and the fused UIOI $R_{F-}^i$ ( (13) ).
Step 3: multi-scale image reconstruction
Obtain the fused image: $\sum_{i=1}^{L-1} R_F^i + G_F^L = F$ .
```

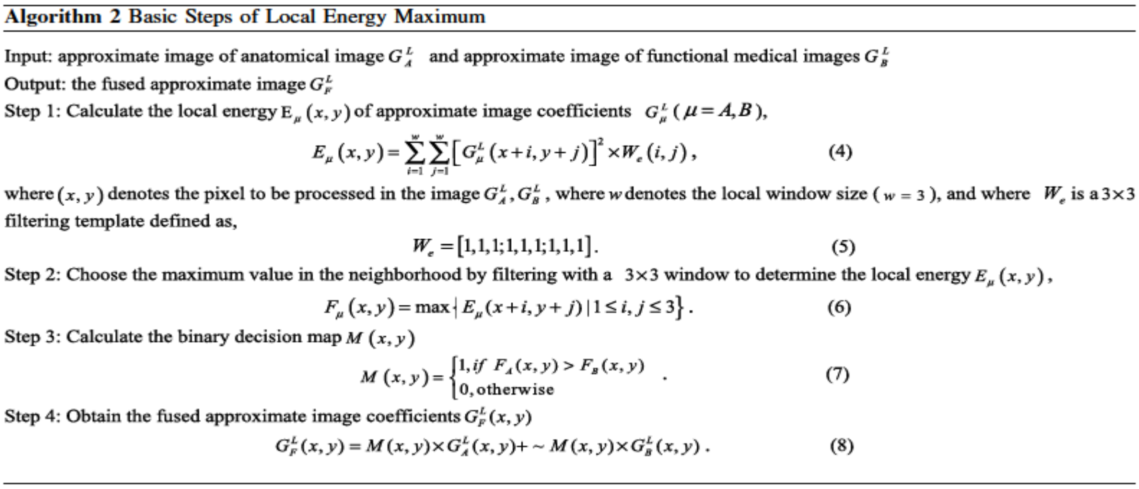
IV. PROPOSED SYSTEM

The main steps of the proposed method for MRI-PET or MRI-SPECT fusion are summarized in Fig. 2 and **Algorithm 1**. In **Algorithm 1**, the proposed fusion method includes three steps: multi-scale image decomposition using LLF, application of image fusion rules using IOI, and multi-scale image reconstruction using the inverse LLF. From Fig. 2, it can be observed that the image fusion rule contains

FuseR and FuseA in the proposed fusion method. FuseR denotes that IOI is used as the image fusion rule for residual images decomposed by LLF, and FuseA denotes that LEM is used as the image fusion rule for approximated images decomposed by LLF.

4.1 Input

The input images are anatomical (MRI) and functional(PET or SPECT) medical imaging data. MRI image, defined as a structural medical image, provides information about the tissue type of the human brain at high spatial resolution. Meanwhile, PET and SPECT images are defined as functional images, providing information on blood flow and biological activity with low spatial resolution. The input images are assumed to be co-registered, which is a common assumption in multi-modal medical image fusion. Let *A* and *B* denote the input anatomical and functional image, respectively.



Algorithm 2 Basic Steps of Local Energy Maximum

Input: approximate image of anatomical image G_A^L and approximate image of functional medical images G_B^L

Output: the fused approximate image G_F^L

Step 1: Calculate the local energy $E_\mu(x,y)$ of approximate image coefficients G_μ^L ($\mu = A, B$),

$$E_\mu(x,y) = \sum_{i=1}^{w}\sum_{j=1}^{w}\left[G_\mu^L(x+i, y+j)\right]^2 \times W_e(i,j), \tag{4}$$

where (x,y) denotes the pixel to be processed in the image G_A^L, G_B^L, where w denotes the local window size ($w = 3$), and where W_e is a 3×3 filtering template defined as,

$$W_e = [1,1,1;1,1,1;1,1,1]. \tag{5}$$

Step 2: Choose the maximum value in the neighborhood by filtering with a 3×3 window to determine the local energy $E_\mu(x,y)$,

$$F_\mu(x,y) = \max\{E_\mu(x+i, y+j) \mid 1 \le i, j \le 3\}. \tag{6}$$

Step 3: Calculate the binary decision map $M(x,y)$

$$M(x,y) = \begin{cases} 1, if\ F_A(x,y) > F_B(x,y) \\ 0, \text{otherwise} \end{cases}. \tag{7}$$

Step 4: Obtain the fused approximate image coefficients $G_F^L(x,y)$

$$G_F^L(x,y) = M(x,y) \times G_A^L(x,y) + \sim M(x,y) \times G_B^L(x,y). \tag{8}$$

4.2 Multi-Scale Image Decomposition

A single image can be decomposed into an approximate image and a series of residual images by LLF. The approximate images *G* provides low-frequency information, such as the basic outline of the brain. Unlike the approximate image, the residual images *R* provide high-frequency information, such as edge information and texture information. In, parameter *L* is the step length in the proposed method. Length *L* is related to subjective and objective evaluations of the fused image. A discussion of length *L* is provided in Section IV.B.

$$A = \sum_{i=1}^{L-1} R_A^i + G_A^L, \quad B = \sum_{i=1}^{L-1} R_B^i + G_B^L.$$

4.3 Image Fusion Rules

Image fusion rules refer to algorithms that seek to highlight features of interest in the original image. Traditionally, image fusion rules contain three components: activity level measurements, coefficient grouping, and coefficient combination,

1) Activity-level measurements: The activity-level scheme measures the salient features of each coefficient at various scales.

2) Coefficient grouping: The coefficient grouping scheme uses a strategy for grouping the corresponding coefficients.

3) Coefficient combination: The coefficient combination aims to combine coefficients at different scales with differently weighted functions.

***1) Local Energy Maximum Based Fusion Rules for Approximate Images**:* The approximate images determined by LLF provide an approximation of the input medical images. Generally, the average (AVG) scheme has been used to fuse the approximate images from the anatomical and functional medical images. However, the resulting fused image introduces ringing artifacts. To pass information within and between each decomposition level to achieve inter-scale dependencies, the fused approximate image should be capable of preserving more low-pass information from the input images. LEM was adopted since it has the advantage of preserving much more regional information using the local energy function in Algorithm 2.

2) Information of Interest Based Fusion Rules for Residual Images:For the residual images, IOI scheme is selected as the fusion rules. It includes two steps:

(1) To obtain IOIs of the residual images: LES and SFare adopted to distinguish the IOI from the un-interest ofinformation (UIOI) For the anatomical image, LES is used to obtain the UIOI with *RiA*¯= LES*(RiA*, *k)* in which the default value of the parameter is *k* = 3. Usually,

the rest of the image is easily obtained by subtracting the UIOI from the input residual images. However, image subtraction using the arithmetic minus operator introduces color distortion because there are many pixel values in the image that are negative. In this study, the subtraction-of-image (SOI) function is defined to obtain the IOI of the residual anatomical image,

$$R^i_{A+}(x,y) = \begin{cases} R^i_A(x,y) - R^i_{A-}(x,y), & \\ & if\ R^i_A(x,y) > R^i_{A-}(x,y) \\ R^i_A(x,y), & \text{otherwise.} \end{cases}$$

For the functional image, SF is adopted as the decomposition scheme for detecting the IOI from the residual functional images (*RiB+ = SF(RiB)*). In addition, the UIOI of the residual functional image is calculated by the SOI function

$$R^i_{B-}(x,y) = \begin{cases} R^i_B(x,y) - R^i_{B+}(x,y), & \\ & if\ R^i_B(x,y) > R^i_{B+}(x,y) \\ R^i_B(x,y), & \text{otherwise.} \end{cases}$$

(2) The fused residual image is obtained as follows. The LEM scheme is chosen for combining decomposed IOIs from the anatomical and functional images. The fused IOI,

$$R^i_{F+} = \begin{cases} R^i_{A+}, & if\ E^i_{A+} > E^i_{B+} \\ R^i_{B+}, & \text{otherwise,} \end{cases}$$

RiF+ is defined as,

where *E* are the pixel values of the local energy defined in with a window size of 3 × 3. The AVG scheme is chosen for combining decomposed UIOIs from the anatomical and functional images. The fused UIOI is defined as,

$$R^i_{F-} = 0.5 \times (R^i_{A-} + R^i_{B-}).$$

Then, corresponding to SOI function, an addition-of image(AOI) function is designed to combine the fused IOI *RiF+* and the fused UIOI *Ri F*−,

$$R^i_F(x,y) = \begin{cases} R^i_{F+}(x,y), & if\ R^i_{F+}(x,y) = R^i_{F-}(x,y) \\ R^i_{F+}(x,y) + R^i_{F-}(x,y), & \\ \quad \text{otherwise.} & \end{cases}$$

4.4. Multi-Scale Image Reconstruction

The fused image is obtained by multi-scale image reconstruction scheme. Fusion methods in the frequency domain usually apply the inverse transform scheme used in multi-scale image decomposition. According to the multi-scale image decomposition shown in , the fused image is obtained using the inverse of equation . Thus, after the fusion of the approximate images and the residual images, the fused images at each scale *i* are combined according to the inverse LLF.

$$\sum_{i=1}^{L-1} R^i_F + G^L_F = F.$$

V. CONCLUSION

In this paper, we propose a new multi-modal medical image fusion method that uses LLF (**Algorithm 1**). In the proposed method, based on the number of levels (*L* = 3), the LLF descriptor is first used to decompose the input anatomical medical images and functional medical images into their multi-scale image representations. Then, the LEM scheme (**Algorithm 2**) is generalized to enable fusing the approximate images. For the decomposed residual images, an IOI-based scheme provides the fusion rule. Finally, the output image is obtained using the inverse LLF. The proposed method is also compared with state-of-the-art fusion methods using ten objective metrics. The proposed method is available in dot net.

REFERENCES

1. R. Singh and A. Khare, “Multiscale medical image fusion in wavelet domain,” Sci. World J., vol. 5, Dec. 2013, Art. no. 521034.
2. N. Chabi, M. Yazdi, and M. Entezarmahdi, “An efficient image fusion method based on dual tree complex wavelet transform,” in Proc. 8th Iranian Conf. Mach. Vis. Image Process., 2013, pp. 403–407.
3. M. Hossny, S. Nahavandi, and D. Creighton, “Comments on ’Information measure for performance of image fusion,”’ Electron. Lett., vol. 44, no. 18, pp. 1066–1067, 2008.
4. W. Xue, L. Zhang, X. Mou, and A. C. Bovik, “Gradient magnitude similarity deviation: A highly efficient perceptual image quality index,” IEEE Trans. Image Process., vol. 23, no. 2, pp. 684–695, Feb. 2014.
5. H. R. Sheikh and A. C. Bovik, “Image information and visual quality,” IEEE Trans. Image Process., vol. 15, no. 2, pp. 430–444, Feb. 2006.
6. H. Yeganeh and Z. Wang, “Objective quality assessment of tone-mapped images,” IEEE Trans. Image Process., vol. 22, no. 2, pp. 657–667, Feb. 2013.
7. L. Liu, B. Liu, H. Huang, and A. C. Bovik, “No-reference image quality assessment based on spatial and spectral entropies,” Signal Process., Image Commun., vol. 29, no. 8, pp. 856–863, 2014.
8. B. Kumar, S. B. Kumar, and C. Kumar, “Development of improved SSIM quality index for compressed medical images,” in Proc. IEEE 2nd Int. Conf. Image Inf. Process. (ICIIP), Dec. 2013, pp. 251–255.
9. S. S. Channappayya, A. C. Bovik, and R. W. Heath, Jr., “Rate bounds on SSIM index of quantized images,” IEEE Trans. Image Process., vol. 17, no. 9, pp. 1624–1639, Sep. 2008.
10. S. Das and M. K. Kundu, “A neuro-fuzzy approach for medical image fusion,” IEEE Trans. Biomed. Eng., vol. 60, no. 12, pp. 3347–3353, Dec. 2013.
11. Z. Xu, “Medical image fusion using multi-level local extrema,” Inf. Fusion, vol. 19, no. 11, pp. 38–48, 2013.

Throughput Evaluation of a Wireless Networks Under Different Kinds of Attacks

Ms. G.Abirami, Ms. M.Arthi, V.Nivetha
UG Students
MRK Institute of Technology, Kattumannarkoil

A.Akilan,
Assistant Professor,
Department of Computer Science and Engineering
MRK Institute of Technology, Kattumannarkoil

Abstract – Denial-of-Service (DoS) is a hazardous* attack *in* a *wireless* network *It's* a *form* of *volumetric* assault. *Anticipated* a *framework to evaluate a network's performance below DoS assault with extraordinary community parameters. Among each community assaults, disbursed Denial of carrier (DDoS) assault is basic to perform, extra detrimental, hard to be traced and tricky to prevent. So, this risk is more serious. The DDoS assault utilizes many unique sources to send a number of vain packets to the goal in a short while, to be able to consume the target's useful source and make the goal's provider occupied. The bots is also both themselves malicious customers that have been preliminarily contaminated (eg., worms and /or Trojans). Applied a novel detecting algorithm for DDoS assaults centered on IP Address Features Value (IAFV) to learn characteristics of a network situated on time lengthen, throughput and packet delivery ratio. The major purpose of the proposed process is to examine the performance metrics under exclusive assaults. In the proposed process, a hybrid algorithm for botnet identification is implemented to explore the network performance on the time of assault. Countless principal parameters including throughput, time lengthen and packet supply ratio are evaluated. Making* use *of* IAFV time series to explain *the state change features of community* glide *along with detecting DDoS attack is* an *identical* way to categorize IAFV *time* sequence. *The proposed approach deploys exclusive nodes* referred *to as DPS nodes. DPS* nodes are used *to monitor the conduct* of *the nodes* in *the community consistently. When the DPS node identifies a node with irregular habits, it's going to announce that node as a wormhole node to the community by using broadcasting a message. All communicative messages shall be deserted by using the network from the wormhole node. The proposed ways are carried out making use of NS2 simulator and the results are mentioned.

Index Terms - **IAFV, Wormhole, Botnet, Support Vector Method**

I. INTRODUCTION

A network especially the Internet is the primary target of the natural attackers' habitat to hide a broad variety of threats. One of the most popular threats is the Denial-of-Service (DoS) attack which can be broadly categorized as a volumetric attack where the target destination is overwhelmed by a huge number of requests eventually leading to the impossibility of serving to any of the users. Distributed Denial-of-Service (DDoS) attacks are usually launched through the botnet, an "army" of compromised nodes hidden in the network. The bots may be either itself malicious users acting consciously or they may be legitimate users that have been preliminarily infected. The existence itself of an anomalous request rate is uncovered and its detection is not an important one. The main challenge is instead ascertaining whether the anomaly is caused by a DDoS attack. If so, performing a correct/early identification of the botnet hidden in the network is a challenging task.

This work suggests three basic things: i) introduce an abstract model for the aforementioned class of attacks, where the botnet emulates normal traffic by continually learning admissible patterns from the environment ii) develop an inference algorithm that is shown to provide a consistent estimate of the botnet possibly hidden in the network iii) verify the validity of the proposed inferential strategy on a test bed environment iv) identify wormhole nodes using Detection and Prevention System nodes v) identify black hole nodes using fake RREP. The test results show that for several scenarios of implementation, the proposed botnet identification algorithm has an observation time of less than one minute to identify correctly almost all bots without affecting the normal users' activity.

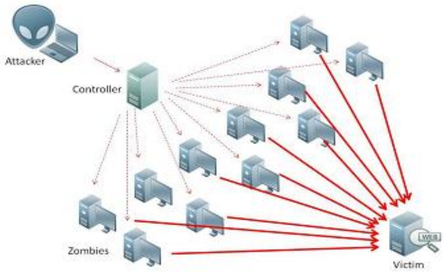


FIGURE1: DOS ARCHITECTURE

II. RELATED WORK

Nazrul Hoque et al. [1] proposes a comprehensive overview of DDoS attacks, their causes, types with a taxonomy and technical details of various attack launching tools. A detailed discussion of several botnet architectures, tools developed using botnet architectures and pros and cons analysis are also included. Furthermore, a list of important issues and research challenges is also reported in the paper.

Laura Feinstein, Dan Schnackenberg et al. [2] presents methods to identify DDoS attacks by computing entropy and frequency-sorted distributions of selected packet attributes. This method describes the detection-response prototype and how the detectors can be extended to make effective response decisions.

Jian Yuan and Kevin Mills et al. [3] propose a method for early attack detection. Using only a few observation points, the proposed method can monitor the macroscopic effect of DDoS flooding attacks. Also shows that such macroscopic-level monitoring might be used to capture shifts in spatial-temporal traffic patterns caused by various DDoS attacks and then to inform more detailed detection systems about where and when a DDoS attack possibly arises in transit or source networks.

Yang Xiang et al. [4] proposes two new information metrics such as the generalized entropy metric and the information distance metric to detect low-rate DDoS attacks by measuring the difference between legitimate traffic and attack traffic. The IP trace back algorithm can find all attacks as well as attackers from their own local area networks (LANs) and discard attack traffic.

Vincenzo Matta et al. [5] propose two strategies to identify the botnet in such challenging scenario, one based on cluster expurgation, the other one on a union rule. Consistency of both algorithms under ideal conditions is ascertained, while their performance is examined over real network traces.

Yih-Chun Hu et al. [6] present a general mechanism, called packet leashes for detecting and defending against wormhole attacks. Presents a specific protocol called TIK that implements leashes. Also discusses topology-based wormhole detection to show that its impossible for these approaches to detect some wormhole topologies.

Mariannne et al. [7] proposes a system in which each node will be assigned a cost depending in its participation in routing. Besides preventing the network from the wormhole attack, the scheme provides a load balance among nodes to avoid exhausting nodes that are always cooperative in routing.

Ming-Yang Su et al. [8] considers link-disjoint multipaths during path discovery and provides greater path selections to avoid malicious nodes, but eventually uses only one path to transmit data. The wormhole nodes would be gradually isolated by their normal neighboring nodes and finally be quarantined by the whole network.

III. PROPOSED SYSTEM

We introduced an abstract model for the DDoS class of attacks, where the botnet emulates normal traffic by continually learning admissible patterns from the environment. Devised an inference algorithm that is shown to provide a consistent (i.e., converging to the true solution as time elapses) estimate of the botnet possibly hidden in the network. Verifying the validity of the proposed inferential strategy on a testbed environment. Tests results show that for several scenarios of implementation, the proposed botnet identification algorithm needs an observation time in the order of less than one minute to identify correctly almost all bots, without affecting the normal users' activity. Implemented a hybrid algorithm for botnet identification to analyze the network performance at the time of attack. Used IAFV time series to describe the state change features of network flow. Detecting the DDoS attack is equivalent to classifying the IAFV time series virtually. Large number of relevant parameters including throughput, time delay and packet delivery ratio are used to test the proposed algorithm.

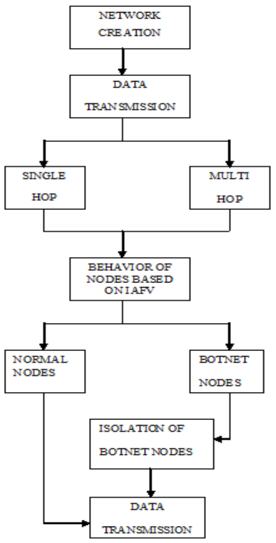


Fig. 3.1 - Data Flow Diagram of the proposed model

The attack flows of DDoS have some features like the abrupt traffic change, flow dissymmetry, distributed source IP addresses and concentrated target IP addresses, etc. In this paper, we propose the concept of IAFV (IP Address Feature Value) to reflect the four features of DDoS attack flow.

$$\mathrm{IAFV}_{\mathrm{F}} = \frac{1}{m}\left(\sum_{i=1}^{m} SIP(SDDi) - m\right)$$

DDoS attack is a kind of attack that sends useless packets to the attack target from many different sources in the hope of exhausting the resources of the target. This act can produce lots of new source IP addresses in a short time, which will lead to an abnormal increase of SIP(SDDi) for some classes of F, that is, the number of different sources to different destination will increase abnormally, causes the flow to be in a quite different state in a short time. The definition of IAFV sums up the different source IP addresses of each SDDi of F in a certain period, then subtract the number of different destination IP addresses m, and divide m at last. So IAFV can reflect the characteristics of a DDoS attack including the burst in the traffic volume, asymmetry of the flow, distributed source IP addresses and a concentrated destination IP address.

3.1. Detection Method Based on IAFV:

To raise the detection rate, decrease the false alarm rate, and enhance the adaptability of detection method, we propose a simple but robust scheme to detect DDoS attacks by extracting IAFV time series from normal flow and DDoS attack flow respectively, and use the SVM (Support Vector Machine) classifier to detect DDoS attacks.

3.2. Anomaly Based Intrusion Detection and Prevention System:

We proposed a Detection and Prevention System (DPS) to identify and square malevolent hubs in MANETs. Exceptional hubs called DPS hubs are sent in the system, which consistently screen the conduct of different hubs. At the point when a DPS hub finds a hub with a suspicious conduct, it announces that suspicious hub as a wormhole hub by communicating a message. All information and control messages are disposed of by the system from a hub that has been announced as wormhole. The quantity of DPS hubs relies on two variables: arrange region and transmission extend. To accomplish best outcomes, DPS hubs ought to be sent such that they cover the entire system region and speak with each other specifically. At whatever point a DPS hub gets a RREQ, course ask for checking begins. As every dp hub keeps record of its neighbors in the Analysis Table, at whatever point it gets a *RREQ* from a hub, it first checks whether the hub that is communicating the RREQ is as of now incorporated into its Analysis Table. In the event that it isn't found in the Analysis Table then another passage is made in which the status is set to dynamic, RREQ check is set to 1.

The Suspicious esteem is set to 0 and Wormhole affirmed fields are set to No. The Suspicious esteem count process checks every one of the hubs in the Analysis Table whose status is dynamic. On the off chance that there is a hub that has RREQ check not as much as Minimum Request Count then its Suspicious esteem is augmented by one. On the off chance that the suspicious esteem is equivalent to Minimum Threat Value and the Wormhole Threat field is No, at that point the DPS hub will communicate a danger message, which incorporates the ID of the vindictive hub. In the wake of sending the Threat message, the Wormhole Threat field of the noxious hub is set to Yes. At that point the procedure will proceed for different hubs. In the event that the suspicious estimation of a hub winds up equivalent to Maximum Threat Value and its Wormhole Confirmed field is No, at that point the DPS hub will communicate a Block message, which contains the ID of the malevolent hub. Subsequent to sending the Block message, the Wormhole Confirmed field is set to Yes. To decrease the false positive rate, if there is a hub that has Suspicious Value more than zero yet indicates typical conduct i.e. the RREQ advances are more than the Minimum Request Count, at that point its Suspicious Value is decremented by one. This condition lessens the odds of genuine hubs being announced as wormhole hubs because of separation from the system. Toward the finish of the Suspicious Value estimation process, the status of the considerable number of hubs in the table is set to dormant and the RREQ Count is set to zero.

IV. EXPERIMENT RESULTS

Tests are performed with nodes & DPS hubs at settled areas utilizing DSDV Protocol. Two noteworthy utilize case situations for wormholes: Fixed wormhole hubs and Mobile wormhole hubs. In the wake of utilizing the DPS hubs, the normal bundle drop rate tumbles too effectively for settled and versatile wormholes separately. There is a considerable amount of lessening in the false positive rate by utilizing the DPS for settled and portable wormhole wormholes, individually when there are 2 wormhole hubs in the system. There is an efficient diminishment in recognition time by utilizing the DPS for settled and versatile wormhole hubs, separately when there are 2 wormhole hubs in the system. The proposed framework performs superior to anything alternate procedures as it doesn't require any unique equipment and isn't influenced by the clog in the system.

V. CONCLUSION AND FUTURE WORK

Distributed Denial of Service (DDoS) attacks launched by bots are capable to learn the application layer interaction possibilities, so as to avoid repeating one simple operation many times. The main contributions of this work are as follows: i) introduced a formal model for the class of randomized DDoS attacks with increasing emulation dictionary ii) proposed an inference algorithm aimed at identifying the botnets executing such advanced DDoS attacks and ascertained the consistency of the algorithm, namely the property of revealing the true botnet as time elapses iii) evaluated the proposed methodologies on a testbed environment. In future, the proposed algorithm can be tested over more datasets in order to examine the impact on performance of the nature of the site under attack. The different behaviors of users surfing on the web can be analyzed. Conducting a refined convergence analysis in order to characterize from an analytical viewpoint, the time needed to reach a prescribed accuracy. The dependence of such time upon the network/botnet size and other relevant system parameters can be taken into considerations.

A detection and prevention system (DPS) against wormhole attacks in Mobile Ad hoc Networks (MANETs) is presented here. The proposed DPS gives the accompanying advantages: I) the ordinary hubs are not influenced i.e. there is no additional preparing required for the identification of vindictive hubs and no additional deferral is included. ii) The danger that a traded off hub spreads bogus data of pronouncing a typical hub as wormhole is limited. iii) The DPS hubs don't partake in ordinary information exchange so their batteries live for longer lengths. The recreations come about demonstrate that the proposed DPS expands the throughput of a system by lessening the parcel drop rate with low false positive rate.

REFERENCES

1. T. He, A. Agaskar, and L. Tong, “Distributed detection of multi-hop information flows with fusion capacity constraints,” IEEE Trans. Signal Processing, vol. 58, no. 6, pp. 3373–3383, Jun. 2010.
2. M. Barni and B. Tondi, “Binary hypothesis testing game with training data,” IEEE Trans. Inf. Theory, vol. 60, no. 8, pp. 4848–4866, Aug.2014

3. M. Barni and F. P´erez Gonz´alez, "Coping with the enemy: advances in adversary-aware signal processing," in Proc. IEEE ICASSP, Vancouver, Canada, May 2013, pp. 8682–8686.
4. M.Barni and B.Tondi,"The source identification game: an information theoretic perspective," IEEE Trans. Inf. Forensics and Security, vol. 8, no. 3, pp. 450–463, Mar. 2013.
5. L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred,"Statistical approaches to DDoS attack detection and response," in Proc. DARPA Information Survivability Conference and Exposition, Washington, DC, USA, Apr. 2003, pp. 303–314
6. S. Ferretti and V. Ghini, "Mitigation of random query string DoS via gossip, and Inf. Sci., vol. 285, pp. 124–134, 2012.
7. T. He and L. Tong, "Detection of information flows," IEEE Trans. Inf. Theory, vol. 54, no. 11, pp. 4925–4945, Nov. 2008.
8. T. He and L. Tong, "Distributed detection of information flows," IEEETrans. Inf. Forensics and Security, vol. 3, no. 3, pp. 390–403, Sep. 2008.
9. N. Hoque, D. Bhattacharyya, and J. Kalita, "Botnet in DDoS attacks: trends and challenges," IEEE Commun. Surveys Tuts.vol.17, no. 4, pp.2242–2270, fourth quarter 2015.
10. B. Kailkhura, S. Brahma, B. Dulek, Y. S Han, and P. Varshney,"Distributed detection in tree networks: Byzantines and mitigation techniques," IEEE Trans. Inf. Forensics and Security, vol. 10, no. 7,pp. 1499–1512, Jul. 2015.
11. J. Kim and L. Tong, "Unsupervised and nonparametric detection of information flows," Signal Processing, vol. 92, no. 11, pp. 2577–2593, Nov. 2012.
12. J. Luo, X. Yang, J. Wang, J. Xu, J. Sun, and K. Long, "On a mathematical model for low-rate shrew DDoS," IEEE Trans. Inf. Forensics and Security, vol. 9, no. 7, pp. 1069–1083, Jul. 2014.
13. S. Marano, V. Matta, T. He, and L. Tong, "The embedding capacity of information flows under renewal traffic," IEEE Trans. Inf. Theory, vol. 59, no. 3, pp. 1724–1739, Mar. 2013.
14. S. Marano, V. Matta, and L. Tong, "Distributed detection in the presence of Byzantine attacks," IEEE Trans. Signal Process, vol. 57, no. 1, pp.16–29, Jan. 2009.
15. S. Marano, V. Matta, and P. Willett, "Distributed detection with censoring sensors under physical layer secrecy," IEEE Trans. Signal Process.,vol. 57, no. 5, pp. 1976–1986, May 2009.
16. M. Mardani and G. B. Giannakis, "Estimating traffic and anomaly maps via network tomography," IEEE/ACM Trans. Networking, DOI: 10.1109 /TNET .2015 .2417809, date of publication, Apr. 2015.
17. M. Mardani, G. Mateos, and G. B. Giannakis, "Dynamic anomalography: tracking network anomalies via sparsity and low rank," IEEE J. Sel. Topics Signal Process., vol. 7, no. 1, pp. 50–66, Feb. 2013.
18. M. Mardani, G. Mateos, and G. B. Giannakis, "Recovery of low-rank plus compressed sparse matrices with application to unveiling traffic anomalies," IEEE Trans. Inf. Theory, vol. 59, no. 8, pp. 5186–5205, Aug. 2013.
19. Matta, M. Di Mauro and M. Longo,"Botnet identification in randomized DDoS attacks," Proc. EUSIPCO, Budapest, Hungary,Aug./Sep.2016, pp.2260–2264.
20. P. Venkitasubramaniam, T. He, and L. Tong, "Anonymous networking amidst eavesdroppers," IEEE Trans. Inf. Theory, vol. 54, no. 6, Jun.2008

Face Recognition and Expression Detection to Aid Visually Impaired People Using Kinect Sensor

Mr. X. Martin Lourduraj,
Assistant Professor,
Department of Computer Science and Engineering,
St. Anne's College of Engineering and Technology.

Mr. E. Veeramani, Mr. M.Mohanraj, Mr. J.Jayavarthanan, Mr. R.Sivamurugan,
UG Students,
Department of Computer Science and Engineering,
St. Anne's College of Engineering and Technology.
.

Abstract – Visually impaired people faces lot of problems in day to day life. Our goal is to make them lead a life which is of security and safety for their own well being. The inability to recognize known individuals in the absence of audio or haptic cues severely restrictions the visually impaired in their social interactions and puts the mat risk from a security view point. Different systems have been developed to aid them so; they can help themselves without the help of second person. In recent years, several prototype systems have been developed to aid this people with the face recognition task. Overview of face recognition system is summarized for aiding the blind and low-vision people. In which one system uses a Microsoft Kinect sensor as a wearable device, performs face detection, and also generates a sound associated with the identified person, virtualized at his/her estimated 3-Dlocation.

Index Terms - **Visually impaired, face recognition, wearable system, system, recognition.**

I.INTRODUCTION

It constitutes an important part of social interaction and human behaviour. Automatic facial expression recognition is a challenging task due to complexity and diversity of facial expressions, inter-person facial differences and the variation of performing facial expression. Therefore, recognizing facial emotion expressions has attracted a great deal of interest by researchers in the last two decades. It has applications in the different fields such as Human Computer Interaction, virtual reality, video games, computer graphics, biometrics, psychology, detecting driver fatigue, analysing customer satisfaction, educational software, lie detection and pain assessment. For the human being, it is easy to recognize facial expressions on the fly, however for computers it is difficult to recognize. This project focus on problem of automatic real time facial expression recognition using distance features for expression classification.

SDK of the Kinect camera is used for face detection and landmark detection. The distance between landmarks is used as features for classification. For finding an optimal subset of features brute force method is used. This optimal subset of features is given as input to the Neural Network. Multilayer perceptron neural network using back propagation algorithm is used for classification of facial expression. The class labels to be recognized are neutral, happy, and surprise facial expressions. For comparison, Lib SVM classifier is used. Previously, no work is available which uses Kinect camera for performing facial landmark detection. Computation time for landmark detection is saved by using Kinect technology.

II. PROPOSED SYSTEM WITH BLOCK DIAGRAM

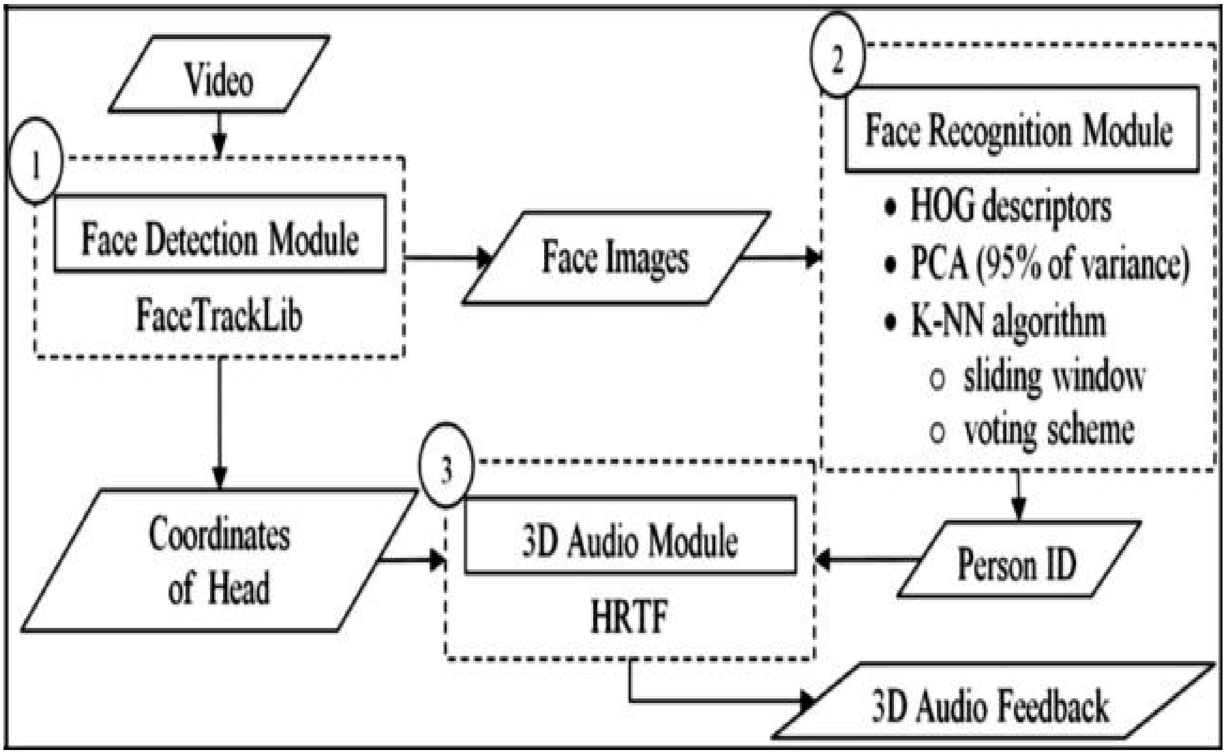


Figure 2.1- Block diagram

2.1 Kinect Based System

According to this system it provides real-time wearable face recognition system. As, it recognizes the face it sends a 3-Daudiofeedback to the user. It provides functionality such as navigation, people localization and recognition, object recognition and the textual information translation. It mainly uses the RGB-Depth technology that comprises of RGB camera to capture color images, an infrared(IR)emitter to emit IR light beams and IR depth sensor to compute the distance between the object and sensor.

2.2 Face Detection

The Face Track Lib uses color, depth, and skeleton information to detect and track human faces in real time. Then, the FDM sends the bounding box around the detected face (i.e., face image—with average size of 64 × 72 pixels) to the FRM. In FRM HOG descriptor shows good result for face identification. The FRM uses Real time face recognition system we use the training set that produced the best accuracy rate in the experiment sliding window size of 60 frames, 48 samples/class in the training set, and K = 1. First, for each frame with a detected face, they compute its HOG descriptor. Next, we centre the descriptor data and multiply it by the PCA rotation matrix in order to reduce its dimensionality. Then, we use the KNN algorithm to classify the sample, and finally, we conduct the voting scheme.

2.3 Face Expression

The first locate the nose, eyes and mouth. Then, from two consecutive normalised frames, a 2D spatio-temporal motion energy representation of facial motion is used as a dynamic face model. use feature points that are automatically tracked using a hierarchical optical flow method. The feature vectors, used for the recognition are created by calculating the displacement of the facial points. The displacement of a point is obtained by subtracting its normalized position in the first frame from its current normalized position. Proposed a feature-based method as mentioned, which uses geometric and motion facial features and detects transient facial features. The extracted features (mouth, eyes, brows and cheeks as) are represented with geometric and motion parameters. The furrows are also detected using a Canny edge detector to measure orientation and quantify their intensity. The parameters of the lower and upper face are then fed into separate neural networks trained to recognize AUs (action units of the facial action coding system). From the history of facial detection by computer vision, we could learn the research process in technology method of facial expression detection: firstly, generate a basic model. Secondly, to locate key points. Thirdly, tacking the movement of key points.

2.4 Hand Gesture

Kinect provides you with the position (X, Y and Z) of the users' joints 30 times (or frames) per second. If some specific points move to specific relative positions for a given amount of time, then you have a gesture. So, in terms of Kinect, a gesture is the relative position of some joints for a given number of frames. Let' s take the **wave** gesture as an example. Visually impaired People wave by raising their left or right hand and moving it from side to side. Throughout the gesture, the hand usually remains above the elbow and moves periodically from left to right. Here is a graphical representation of the movement. the wave gesture, the hand remains above the elbow and moves periodically from left to right. Each position (left / right) is a discrete part of the gesture. Formally, these parts are called segments.

2.5 Text To Speech

Finally recognized human name is announced using Letter to Sound (LTS) type speech synthesis technique. The real-time system returns the 3-D audio feedback of the identified person every 60 votes, achieving a frame rate close to 30 frames/s.

III. TECHNIQUES

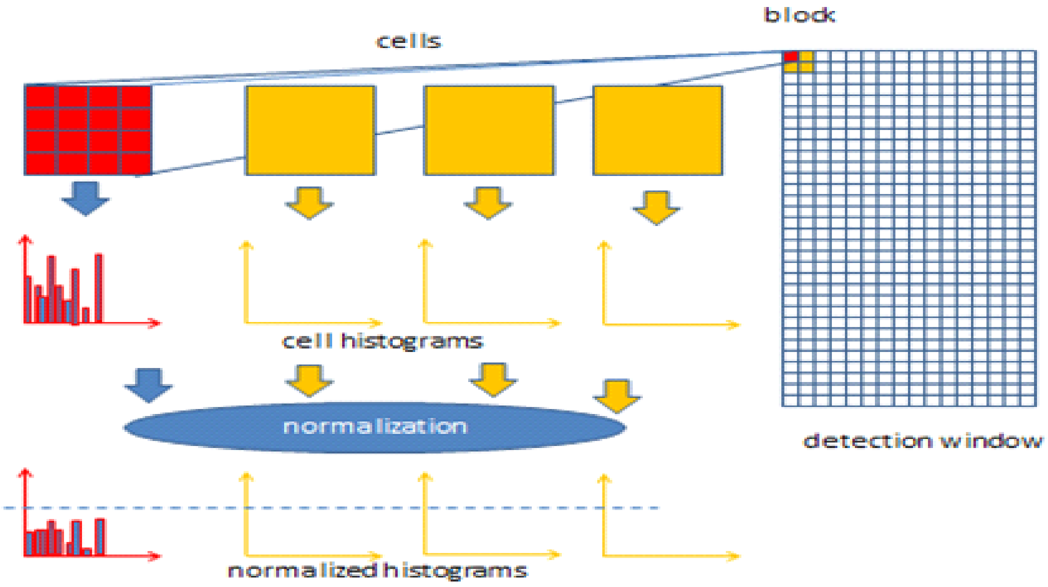
3.1 Histogram Of Oriented Gradients (HOG)Algorithm

Descriptor Histogram of oriented gradients (HOG) is a feature descriptor used to detect objects in computer vision and image processing. The HOG descriptor technique counts occurrences of gradient orientation in localized portions of an image - detection window, or region of interest (ROI).Implementation of the HOG descriptor algorithm is as follows:

- Divide the image into small connected regions called cells, and for each cell compute a histogram of gradient directions or edge orientations for the pixels within the cell.
- Discretize each cell into angular bins according to the gradient orientation.

- Each cell's pixel contributes weighted gradient to its corresponding angular bin.
- Groups of adjacent cells are considered as spatial regions called blocks. The grouping of cells into a block is the basis for grouping and normalization of histograms.
- Normalized group of histograms represents the block histogram. The set of these block histograms represents the descriptor.

The following figure demonstrates the algorithm implementation scheme:



Computation of the HOG descriptor requires the following basic configuration parameters:

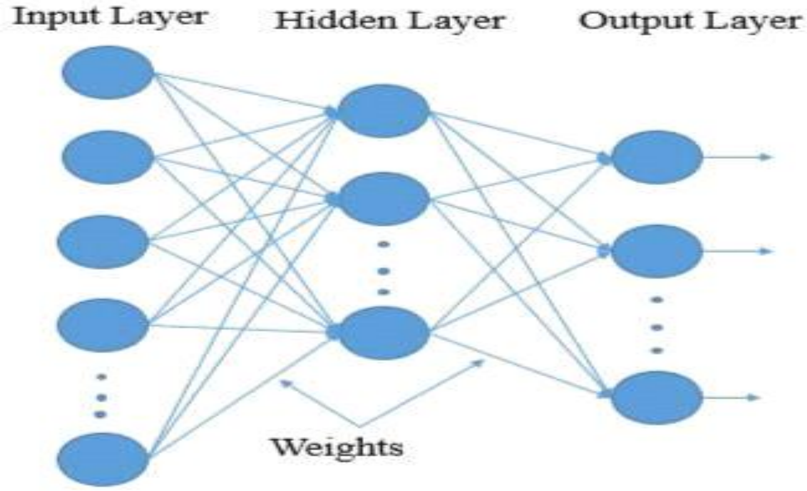
- Masks to compute derivatives and gradients
- Geometry of splitting an image into cells and grouping cells into a block
- Block overlapping
- Normalization parameters

3.2 Support Vector Machine (SVM) Algorithm

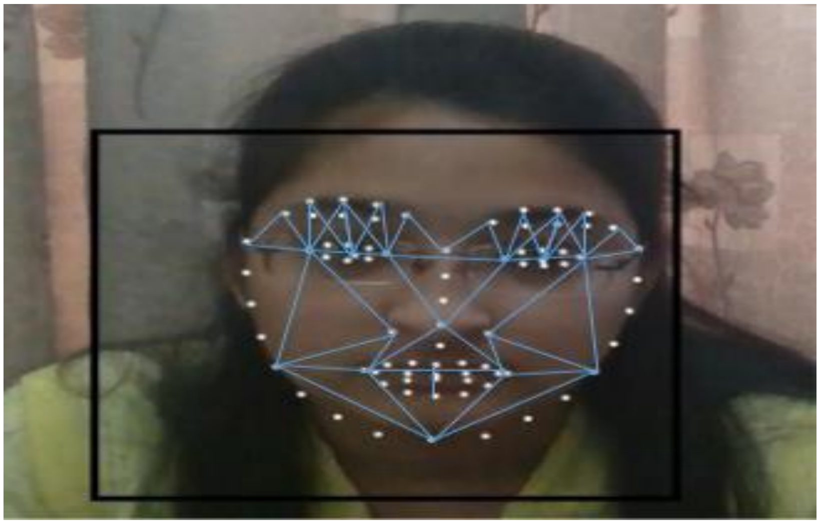
In machine learning, support vector machines (SVMs, also support vector networks) are supervised learning models with associated learning algorithms that analyse data used for classification and regression analysis. Given a set of training examples, each marked as belonging to one or the other of two categories, an SVM training algorithm builds a model that assigns new examples to one category or the other, making it a non-probabilistic binary linear classifier.

3.3 Multi-Layer Perceptron (MLP) Algorithm

Multi-Layer Perceptron (MLP) neural network is supervised learning algorithm which is used for classification and pattern recognition. The proposed system uses MLP neural network as a classifier. Standard back-propagation algorithm is used as a learning algorithm. It consists of input layer, hidden layer, and output layer. The number of input neurons is equal to the number of selected features. Similarly, the number of output neurons is equal to the number of facial expressions to be recognized. Here, a number of output neurons is three i.e. for class neutral, happy, and surprise. The input layer neurons are connected to the hidden layer neurons and the hidden layer neurons are connected to output layer neurons in which each connection has a weight associated with it shows the general architecture of MLP neural network.



IV. OUTPUT MEASURES



V. CONCLUSION

Overview of different system has been summarized to resolve the problems of visually impaired people. Mainly, the face recognition systems help to solve real time problems i.e. people recognition and face recognition. The iCare Inter action Assistant uses the algorithms such as PCA and LDA. The algorithms are the be stones for providing face images. A Kinect wearable face recognition system uses RBG-Dimage, as an efficient algorithm to detect faces in all direction. Never the less, several issues are still needed to be addressed.

REFERENCES

1. Ekman and W. V. Friesen, "Measuring facial movement, "Environmental Psychology and Nonverbal Behavior, vol. 1,no. 1, pp. 56–75,1976
2. Boqing Gong, Yueming Wang, Automatic facial expression recognition on a single 3D face by exploring shape deformation, in MM '09 Proceedings of the 17th ACM international conference on Multimedia, pages 569-572
3. Rabiuet al.: 3D facial expression recognition using maximum relevance minimum redundancy geometrical features. EURASIP Journal on Advances in Signal Processing 2012 2012:213. doi:10.1186/1687-6180-2012-213
4. Mingliang Xue; Mian, A.; Wanquan Liu; Ling Li, "Fullyautomatic 3D facial expression recognition using local depth features," in Applications of Computer Vision (WACV), 2014 IEEE Winter Conference on , vol., no., pp.1096-1103, 24-26 March 2014. doi: 10.1109/WACV.2014.683
5. Razuri, J.G.; Sundgren, D.; Rahmani, R.; Moran Cardenas, A., "Automatic Emotion Recognition through Facial Expression Analysis in Merged Images Based on an Artificial Neural Network," in Artificial Intelligence (MICAI), 2013 12th Mexican International Conference on , vol., no., pp.85-96, 24-30 Nov. 2013. doi: 10.1109/MICAI.2013.16

Android Based Position Detecting and Tracking System Using GPS and GSM

Mrs.M.Senthamarai Selvi
Associate Professor
Department of Computer Science and Engineering,
St.Anne's College of Engineering and Technology

Ms.K.Anusuya, Ms.J.Jayasri, Ms.S.Manju, Ms. A.Yuvasri
UG Students
Department of Computer Science and Engineering,
St.Anne's College of Engineering and Technology

Abstract - Today's fast moving services based on location are very much important. As the trend is of smartphones, iphones and the emerging gadgets, it is very important for the user to have location based services. The location based services are accompanied with the help of GPS(Global Positioning System) and GSM(Global System for Mobile communication). GPS and GSM technologies with Google earth to provide real-time data have also been proposed Global positioning systems and mobile phone networks make it possible to track individual users with an increasing accuracy. The application will allow the user to locate friends dynamically and can also communicate with them easily and effectively and will also locate the friends on Google Maps.

Keywords- Global Positioning System (GPS),Global System for Mobile communication(GSM),Google Maps, Retrofit.

I. INTRODUCTION

Various GPS-based tracking systems have been successfully deployed and utilized in various applications such as fleet and vehicle location identification, and in route guidance. Recently, systems that integrate GPS and GSM technologies with Google earth to provide real-time data have also been proposed Global positioning systems and mobile phone networks make it possible to track individual users with an increasing accuracy. "GPS based Location Tracker" is a GPS service based application which would help us in locating the exact geo-position of people (any single entity of a large set) depending upon their current location where abouts. Geo-position would be displayed on the map view on our android set and display functioning can analogue to the current usage of Google Maps / Nokia Maps / iOS Map Service.In our application, we have used Map Views as supported by Google APIs.

II. LITERATURE REVIEW

The following paper presents a system used to track or locate nearest friends locations and get constant updates about the same with an effective communication with the friends.

[1]. Arnon Amir in "Buddy tracking — efficient proximity detection among mobile friends" present an approach to maintain information about social sites using dynamic coordinates using centralized and peer-to-peer servers.

[2].F. Aloul in “Using Mobiles for On Campus Location Tracking” presents an approach that shows the implementation of a simple and cost effective system that assists users in tracking colleagues and friends within a campus environment.

[3].Ruchika Gupta in “GPS and GPRS Based Cost Effective Human Tracking System Using Mobile Phones” presents an approach that the whole system allows the user's mobility to be tracked using a mobile phone which is equipped with an internal GPS receiver and a GPRS transmitter. A mobile phone application has been developed and deployed on an Android Phone whose responsibility is to track the GPS location and send it to a remote location by creating a GPRS packet.

[4]. R.Anand G in “Mitter – Bitter Monitoring System Using Android Smartphone’s” presents an approach Employee monitoring system using android mobile is, essentially, software that allows Managers to monitor their Employee's office cell phone.

III. SYSTEM ARCHITECTURE

The architecture depicted in Figure 1 decomposes the system into various components that seamlessly interact providing a practical solution to the positioning problem . The system follows a typical client/server architecture with the client (mobile) running an application specifically built for this project.

3.1. Server

The server functions were implemented using PHP scripts. The server is the hardcore of the system. The main tasks of PHP server are: register users, update the database, retrieve user location, sends out user location information via SMS and post it online.

3.2.Application

On the mobile side, the application was developed and implemented using Java 2 micro edition (J2ME) . The J2ME application runs on any Symbian OS based phone. Note that the application can only operate on a WiFi- enabled mobile phone.

3.3.Database

The server uses a MySQL database. MySQL is an open source relational database management system which uses Structured Query Language (SQL). MySQL was chosen because of its reliability, speed and flexibility. The server receives requests from the application program. The request can be either to register a new user, update user information, or locate an existing user. The server tokenizes the user requests, and issues the appropriate SQL statement to perform the required action.

IV. PROPOSED SYSTEM

We are going to use GPS for locating the position of mobile. We will also find the accurate position of user in real time. We can track mobile through android application using GPS to find out here a bus is using a web application which requires login of administrator for mobile Details and User. We use the mobile details From mobile Registration Form i.e. (user Name, user No,Password,Address.).This is the Administrative Activity. From that detail we can track the location of user, only registered user location can track friends and family

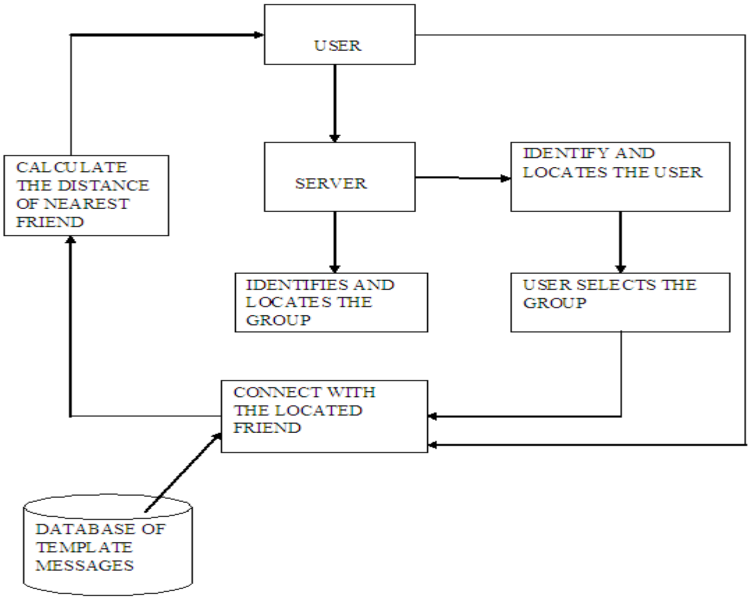

USER
SERVER
IDENTIFY AND LOCATES THE USER
CALCULATE THE DISTANCE OF NEAREST FRIEND
IDENTIFIES AND LOCATES THE GROUP
USER SELECTS THE GROUP
CONNECT WITH THE LOCATED FRIEND
DATABASE OF TEMPLATE MESSAGES

Figure 4.1 - Proposed system

As shown in Figure1. The system starts with the identification and authentication of the user with the server. The user first sends request to the server for connection with the server to locate friends. The server returns an validation to user confirming his/her request. The user is then allowed to select the group of friends which are to be located on the map(Google map). After the selection of the group the server again identifies the selected group of friends and confirms the users request. The group is then searched with the use of GPS and GPRS and also the geographical coordinates. After the group is been located each and every located friend's distance is calculated with the user to identify who is closest to the user. After the calculation of distances the system will generate the result only for friends who are nearest to the user. The minimum nearest distance can be feeded by the user and the system will locate friends accordingly. After the location of nearest friends is done the user may select any of the friends from the located ones to send a template message from the database.

V. REQUIREMENTS

5.1 Hardware Requirement

The proposed system requires an Android phone(version above 4.0) or an emulator(Micro emulator 5055) for executing the application i.e it will provide the platform for the application to run.

5.2 Software Requirement

In the proposed system we will be using Android sdk 1.2 or above for the device that we will use, at the front end we will be using java for developing the application using Eclipse IDE(3.4) tool and for interfacing with the user.

5.3 Database

We will be using MySQL Server for the database as message templates is to be stored in database also the location updates of ever y located friend is to be stored.

VI. CONCLUSION

This paper provides a mobile tracking application based on GPS and it uses geographical co-ordinates of the user to locate the mobile device. This application also ensures the effective calculation of the distance between the user and the located friends resulting interest being shown to the ones who are nearest to the user. The main objective is to track the location and send SMS to the selected ones. As the location tacking services are emerging with a good popularity this application will be a good criterion for it.

VII. FUTURE SCOPE

Android technology (OS) is the base technology and it is user friendly as it is a Linux product and is also secure. Android based products reduces cost as Android is an open source product allowing easy compatibility of applications. The communication provider provides with a methodology that need not be changed and can be directly agreed to confirm a protocol to exchange location messages. In general, battery drainage of small mobile devices resulting from communications is far more significant than the energy needed for computing**.** The peer-to peer model minimizes the number of location update messages sent by the user, on the expense of the much -less-costly increase of computation cost. Availability includes the automatic updates provided so that it becomes a task at the users end. Whether the user wants to or doesn't want updates in the system. Featuring will be available with improving versions. The system can be used with different OS devices too as the product will have a base of Android which itself is an Open source OS. Also, it is provided with the property of user friendliness and easy compatibility.

REFERENCES

1. Abhijeet Tekawade, Ahemad Tutake, Ravindra Shinde, Pranay Dhole,Mr. Sumit Hirve, “Mobile Tracking Application for Locating Friends using LBS”, April 2013.
2. Arnon Amir, Alon Efrat, Jussi Myllymaki, Lingeshwaran Palaniappan, Kevin Wampler, “Buddy tracking — efficient proximity detection among mobile friends”,2004.
3. F. Aloul, A. Sagahyroon, A. Al-Shami, I. Al-Midfa, R. Moutassem, “Using Mobiles for On Campus Location Tracking”.
4. Ruchika Gupta and BVR Reddy, “GPS and GPRS Based Cost Effective Human Tracking System Using Mobile Phones”, January-June 2011.
5. R.Anand G. Arun Kumar S.Murthy “Mitter – Bitter Monitoring System Using Android Smartphone's” ,2010.

Secure and Efficient Access Control Over P2P Cloud Storage System

Mrs.A.Sudha
Student,
Department of Computer Science and Engineering,
Krishnasamy College of Engineering and Technology

Mrs. PM. Kamatchi , Ms.Sivaranjini
Assistant Professor,
Department of Information and Technology,
Krishnasamy College of Engineering and Technology

Abstract - With the popularity of outsourcing data to the cloud, it is important to protect the privacy of data. A P2P storage cloud can be formed to offer highly available storage services, lowering the economic cost by exploiting the storage space of participating users. However, since cloud severs and users are usually outside the trusted domain of data owners, P2P storage cloud brings forth new challenges for data security and access control when data owners store sensitive data for sharing in the trusted domain. Moreover, there are no mechanisms for access control in P2P storage cloud. To address this issue, this project propose design a cipher text-policy attribute-based encryption () scheme and a proxy re-encryption scheme. Based on them, further propose a secure and efficient access control over peer to peer cloud storage system. This project enforces access policies based on user attributes, and integrate P2P reputation system. This enables data owners to delegate most of the laborious user revocation tasks to cloud servers and reputable system peers. Our security analysis demonstrates that system is provably secure.

Index Terms – ***P2P, cloud computing, ABE scheme***

I. INTRODUCTION

Cloud computing is an on demand service in which shared resources, information, software and other devices are provided according to the clients requirement at specific time. It's a term which is generally used in case of Internet. The whole Internet can be viewed as a cloud. Capital and operational costs can be cut using cloud computing.

Security is one of the main user concerns for the adoption of Cloud computing. Moving data to the Cloud usually implies relying on the Cloud Service Provider (CSP) for data protection. Although this is usually managed based on legal or Service Level Agreements (SLA), the CSP could potentially access the data or even provide it to third parties. Moreover, one should trust the CSP to legitimately apply the access control rules defined by the data owner for other users. The problem becomes even more complex in Inter cloud scenarios where data may flow from one CSP to another. Users may loss control on their data. Even the trust on the federated CSPs is outside the control of the data owner. This situation leads to rethink about data security approaches and to move to a data-centric approach where data are self-protected whenever they reside.

Load balancing in cloud computing systems is really a challenge now. Always a distributed solution is required. Because it is not always practically feasible or cost efficient to maintain one or more idle services just as to fulfill the required demands. Jobs can't be assigned to appropriate servers and clients individually for efficient load balancing as cloud is a very complex structure and components are present throughout a wide spread area. Here some uncertainty is attached while jobs are assigned.

II. LITERATURE REVIEW

Hung He, Ruixuan Li, Xinhua Dong, and Zhao Zhang suggested the technique preliminaries closely related to ACPC, and then present the system model and some security assumptions of ACPC. At a high level, our work is similar to the recent work. attribute based encryption (KP-), however it require substantially new techniques. In key-policy attribute based encryption, cipher texts are associated with sets of descriptive attributes, and user keys are associated with policies (the reverse of our situation).

P. Mell and T. Grange suggesting an alogorithm that in key-policy , the encrypted exerts no control over who has access to the data she encrypts, except by her choice of descriptive attributes for the data. Rather, she must trust that the key -issuer issues the appropriate keys to grant or deny access to the appropriate users. In other words, in the intelligence" is assumed to be with the key issuer, and not the encrypted. In our setting, the encryption must be able to intelligently decide who should or should not have access to the data that she encrypts and present a system for realizing complex access control on encrypted data that it call Cipher text -Policy Attribute-Based Encryption. By using our techniques encrypted data can be kept confidential even if the storage server is un trusted; moreover, our methods are secure against collusion attacks. Rodrigues and P. Rachel for proposing Attribute-Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt.

III. EXISTING SYSTEM

This project presents SecRBAC, a data - centric access control solution for self – protected data that can run in untrusted CSPs and provides extended Role - Based Access Control expressiveness. The proposed authorization solution pro-vides a rule- based approach following the RBAC scheme, where roles are used to ease the management of access to the resources. This approach can help to control and manage security and to deal with the complexity of man-aging access control in Cloud computing. Role and resource hierarchies are supported by the authorization model, pro-viding more expressiveness to the rules by enabling the definition of simple but powerful rules that apply to several users and resources thanks to privilege propagation through roles and hierarchies. Policy rule specifications are based on Semantic Web technologies that enable enriched rule definitions and advanced policy management features like conflict detection.

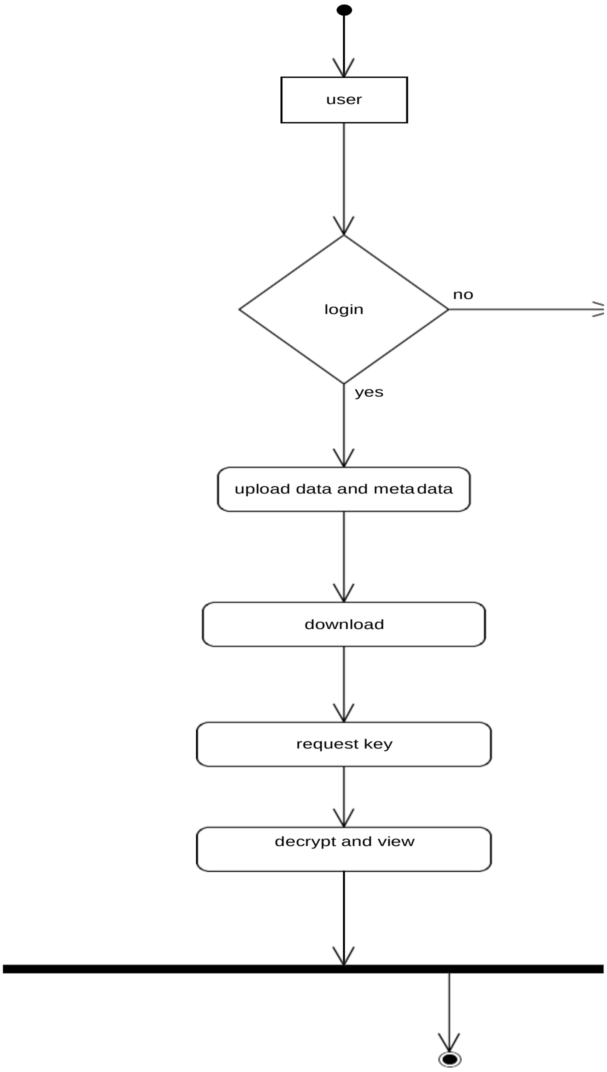
A data-centric approach is used for data self-protection, where novel cryptographic techniques such as Proxy Re-Encryption (PRE), Identity-Based Encryption (IBE) and Identity-Based Proxy Re-Encryption (IBPRE) are used. They allow to re-encrypt data from one key to another without getting access and to use identities in cryptographic operations. These techniques are used to protect both the data and the authorization model. Each piece of data is ciphered with its own en-crypt ion key linked to the authorization model and rules are cryptographically protected to preserve data against the service provider access or misbehavior when evaluating the rules. It also combines a user-centric approach for authorization rules, where the data owner can define a unified access control policy for his data. The solution enables a rule- based approach for authorization in Cloud systems where rules are under control of the data owner and access control computation is delegated to the CSP, but making it unable to grant access to unauthorized parties.

The contributions of existing system as follows Data-centric solution with data protection for the Cloud Service Provider to be unable to access it.

- Rule-based approach for authorization where rules are under control of the data owner.

- High expressiveness for authorization rules applying the RBAC scheme with role hierarchy and resource hierarchy (Hierarchical RBAC or HRBAC).
- Access control computation delegated to the CSP, but being unable to grant access to unauthorized parties.

IV. METHODOLOGY OF THE WORK

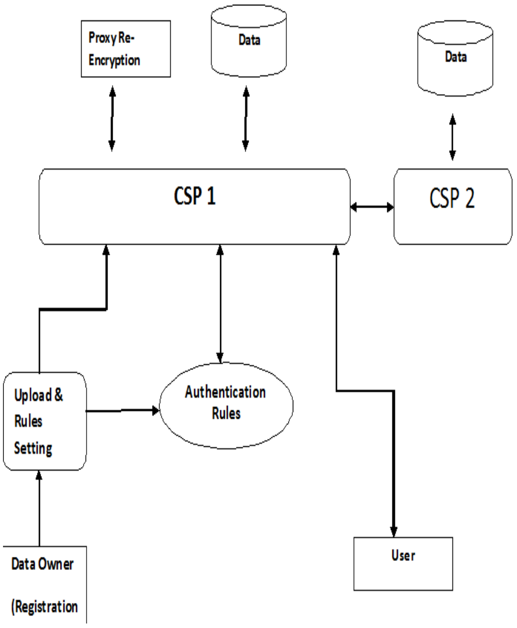


V. PROPOSED SYSTEM

In this approach design a cipher text- policy attribute-based encryption () scheme and a proxy re-encryption scheme. Based on them, this project further proposes a secure and efficient access control over peer to peer cloud storage system. Here with enforce access policies based on user attributes, and integrate P2P reputation system. This enables data owners to delegate most of the laborious user revocation tasks to cloud servers and reputable system peers.

Architecture is also proposed for the deployment within CSPs. This architecture takes into consideration the different elements that should be deployed in order to give an overview of how access to protected data is done in this approach. When moving data to the cloud, a self- protected package is generated by the data owner. This package contains: the encrypted data objects, the authorization rules and the corresponding re-encryption keys. Data objects are encrypted before uploading them to the Cloud in order to prevent the CSP to access them. This is done by data owners by using the encrypt () function.

Data should be encrypted using the identity ido1 of the object being uploaded o1. A digital envelope approach can be applied to protect data objects instead of direct encryption. This would enhance cryptographic operations like re encryptions for large data objects. This approach consists in using a symmetric encryption algorithm (e.g. AES) to protect the data object itself. The encryption of data is done with a random symmetric key generated for the purpose of a double encryption.. Authorization rules are defined by the data owner and directly mapped into the authorization model. This is done by including the corresponding elements in the binary relations. For instance, a rule that grants a subject s1 access to an object o1 would add an element g1 = (s1; o1) to the binary relation.



Regarding the CSP, there are two main modules to be deployed: a Policy Decision Point (An authorization service (AuthzService) acts as entry point to the PDP for Cloud services allowing querying it for authorization decisions. This module takes decisions upon a request from a user s1 to access to a piece of data o1 managed by the service. These decisions usually return an access granted or denied statement. The results of this module are processed by the AuthzService to form an authorization decision. In case ofa positive decision, it also obtains the corresponding authorization chain and the re-encryption keys for such a chain.

Here with design a cipher text- policy attribute-based encryption () scheme and a proxy re-encryption scheme. Based on them, this project further proposes a secure and efficient access control over peer to peer cloud storage system. This Project enforces access policies based on user attributes, and integrate P2P reputation system. This enables data owners to delegate most of the laborious user revocation tasks to cloud servers and reputable system peers.

- Proposed system allows authenticated users to modify and delete data.
- Suitable for peer to peer cloud storage system without breaking the existing security policies.

VI. CONCLUSION

This paper aims at providing secure, efficient and fine grained data access control in P2P storage cloud. To achieve this goal, design an efficient ABE scheme and a corresponding PRE scheme. To efficiently address the issue of user revocation, in Access control over p2p cloud storage system(ACPC). Process integrate P2P reputation system and enable the data owner to delegate file re encryption to cloud servers and delegate user secret key update, the most computation intensive task, to the reputable system peers picked out by P2P reputation system. Moreover, ACPC is provably secure under the standard security model and can resist collusion attacks and protect user access privilege information effectively.

REFERENCES

1. B. Balamurugan and P. Venkata Krishna,(2014) "Extensive survey on usage of attribute based encryption in cloud," Journal of Emerging Technologies in Web Intelligence, vol.6, no.3.
2. Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing v3.0," CSA, Tech. Rep., 2003.
3. Hung He, Ruixuan Li, Xinhua Dong, and Zhao Zhang ”Secure, Efficient and Fine - Grained Data Access Control Mechanism for P2P Storage Cloud” IEEE transactions oncloud computing, vol. 2, no. 4.
4. InterNational Committee for Information Technology Standards, (2014)"INCITS 494- information technology - role based access control - policy enhanced," INCITS, Standard.
5. Martin Randles, David Lamb, A. Taleb-Bendiab,(2010) A Comparative Study into Distributed Load Balancing Algorithms for Cloud Computing,IEEE 24th International Conference on Advanced Information Networking and Applications Workshops.
6. P. Mell and T. Grange, ”The NIST definition of cloud computing, NIST S pecial800-145, Sep.(2011)

Image-Text Matching Tasks Using Two Branch Neural Networks

Mr. S. Rajarajan,
Assistant Professor,
Department of Computer Science and Engineering,
St. Anne's College of Engineering and Technology, Panruti.

Ms. M. Abina, Ms. S. Srimathi
UG Students
Department of Computer Science and Engineering,
St. Anne's College of Engineering and Technology, Panruti.

Abstract - Image-language matching tasks have recently attracted a lot of attention in the computer vision field. These tasks include image-sentence matching, i.e., given an image query, retrieving relevant sentences and vice versa, and region-phrase matching or visual grounding, i.e., matching a phrase to relevant regions. This paper investigates two-branch neural networks for learning the similarity between these two data modalities. We propose two network structures that produce different output representations. The first one, referred to as an embedding network, learns an explicit shared latent embedding space with a maximum-margin ranking loss and novel neighborhood constraints. Compared to standard triplet sampling, we perform improved neighborhood sampling that takes neighborhood information into consideration while constructing mini-batches. The second network structure, referred to as a similarity network, fuses the two branches via element-wise product and is trained with regression loss to directly predict a similarity score. Extensive experiments show that our networks achieve high accuracies for phrase localization on the Flickr30K Entities dataset and for bi-directional image-sentence retrieval on Flickr30K and MSCOCO datasets.

Index terms — Deep Learning, Cross-Modal Retrieval, Image-Sentence Retrieval, Phrase Localization, Visual Grounding.

I. INTRODUCTION

Computer vision is moving from predicting discrete, categorical labels to generating rich descriptions of visual data, in particular, in the form of natural language. We are witnessing a surge of interest in tasks that involve cross-modal learning from image and text data, widely viewed as the "next frontier' of scene understanding. For example, in bi-directional image-sentence search one aims to retrieve the corresponding images given a sentence query, and vice versa. Image captioning is the task of generating a natural language description of an input image. Motivated by the notion of creating a visual Turing test, Visual Question Answering (VQA) aims at answering freeform questions about image content. Visual grounding tasks like referring expression understanding and phrase localization find image regions indicated by questions, phrases, or sentences. To support these tasks, a number of large-scale datasets and benchmarks have recently been proposed, including MSCOCO and Flickr30K datasets for image captioning, Flickr30K Entities for phrase localization, the

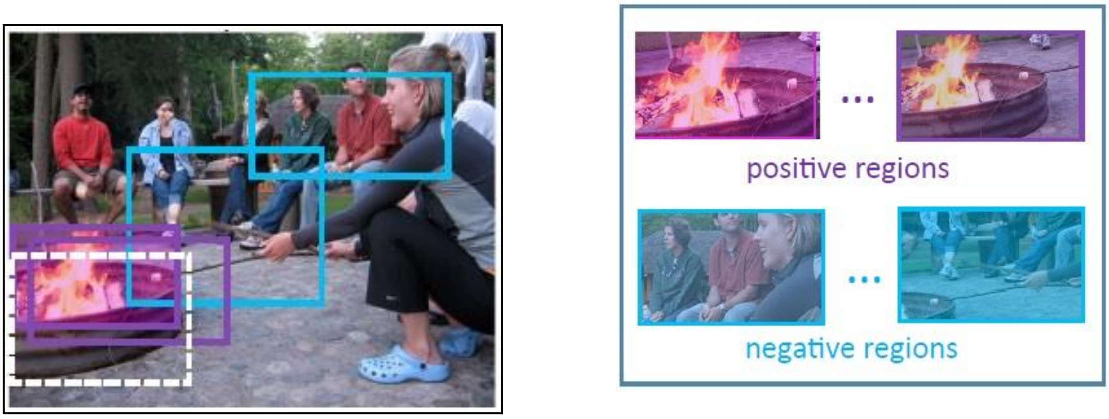


Fig. 1. A group of eight campers sit around a fire pit . Taking the phrase localization task as an example, we show the architectures of the two-branch networks used in this paper. It gives the phrase "a fire pit" from the image caption, sets of positive regions (purple) and negative regions (blue) are extracted from the training image. The positive regions are defined as ones that have a sufficiently high overlap with the ground truth (dashed white rectangle).

Visual Genome dataset for localized textual description of images, and the VQA dataset for question answering. We study neural architectures for a core problem underlying most image-text tasks--how to measure the semantic similarity between visual data, e.g., images or regions, and text data, e.g., sentences or phrases. Learning this similarity requires connecting low-level pixel values and high-level language descriptions. Figure 1 shows an example of a phrase description of an image region from the Flick30K Entities dataset. Matching the phrase "fire pit" to its corresponding region requires not only distinguishing between the correct region and background clutter, but also understanding the difference between "fire pit" and other visual concepts that might be present in the image. Naively, one might consider training binary or multi-class classifiers to estimate the probabilities of various concepts given image regions. However, the natural language vocabulary of visual concepts is very large, even if we restrict these concepts to nouns or simple noun phrases. Further, different concepts have complex semantic similarity relationships between them –for example, "fire" and "flame" are synonyms, "fireplace" is similar in meaning but not identical to "fire pit," and attributes can modify the meaning of head nouns ("fire pit" is not the same as "pit"). This suggests that, instead of representing different phrases using separate classifiers, representing text in a continuous "semantic" embedding space is more appropriate. Furthermore, the frequencies of different phrases are highly unbalanced: the word "fire" only occurs three times in the Flickr30K Entities dataset, while the most common words, such as "man," show up a few hundred times. For all these reasons, training separate per-concept classifiers is undesirable .

As suggested by the above discussion, the network architecture for these tasks should consist of two branches that take in image and text features respectively, pass them through one or more layers of transformations, fuse them, and eventually output a learned similarity score. At a conceptual level, there are two ways to obtain this score. One is to train the network to map images and text into an explicit joint embedding space in which corresponding samples from the two modalities lie close to one another, and image text similarity is given by cosine similarity or Euclidean distance. The second approach is to frame image/text correspondence as a binary classification problem: given an image/text pair, the goal is to output the probability that the two items match. Accordingly, we propose two variants of two-branch networks that follow these two strategies ***the embedding network*** and ***the similarity network.***

Embedding Network: The goal of this network is to map image and text features, which may initially have different dimensions, to a joint latent space of common dimensionality in which matching image and text features have high cosine similarity. We train the network with a bi-directional ranking loss than enforces that matched sample pairs should have smaller distance than unmatched ones in the embedding space.

Similarity Network: In our alternative architecture, image and text data is also passed through branches with two layers with nonlinearities, but then, element-wise product is used to aggregate features from the two branches into a single vector, followed by a further series of fully connected layers. This network is trained with logistic regression loss to match the output score to +1 for positive pairs and -1 for negative pairs. Our contributions can be summarized as follows:

❖ We propose state-of-the-are embedding and similarity networks for learning the correspondence between image and text data for two tasks: phrase localization (given a phrase, find a corresponding bounding box in the image) and bi-directional image-sentence search (given a query image/sentence, retrieve matching sentences/images from a database).

❖ We systematically investigate all important components of both embedding and similarity networks, including loss functions, feature fusion strategies, and different ways of sampling positive and negative examples to form mini-batches during training.

❖ We obtain state-of-the-art accuracies on phrase localization on the Flickr30K Entities dataset and near state-of-the-art accuracies on bi-directional image-sentence retrieval on Flickr30K and MSCOCO datasets.

Our two-branch networks are very general and can be modified and applied to other image-text tasks.

II. RELATED WORK

CCA-based methods. One of the most popular baselines for image-text embedding is Canonical Correlation Analysis (CCA), which finds linear projections that maximize the correlation between projected vectors. To obtain a nonlinear embedding, other works have opted for kernel CCA which finds maximally correlated projections in reproducing kernel Hilbert spaces with corresponding kernels. Despite being a classic textbook method, CCA has turned out to be a surprisingly powerful baseline[1].The main disadvantage of CCA is its high memory cost, as it requires loading all the data into memory to compute the data covariance matrix.

Deep multimodal representations. To extend CCA to learning nonlinear projections and improve its scalability to large training sets, Andrew et al. [2] and Yan and Mikolajczyk [3] proposed to cast CCA into a deep learning framework. Their methods are trained using stochastic gradient descent (SGD) and thus can be applied to large-scale datasets. SGD cannot guarantee a good solution to the generalized eigen value problem at the heart of CCA because covariance estimation in each mini batch is unstable. Our proposed networks share a similar two-branch architecture with deep CCA models, but they are much more stable and accurate.

Ranking-based methods. Some of the most successful multi-modal methods, whether they be linear models or deep networks, are trained with a ranking loss. For example, WSABIE [4] and DeVISE [5] learn linear transformations of visual and text features into a shared space using a *single-directional* ranking loss, which applies a margin-based penalty to an incorrect annotation when it gets ranked higher than a correct one for describing an image. A *bi-directional* ranking loss adds the missing link in the opposite direction: It further ensures that for each annotation, the corresponding image gets ranked higher than unrelated images. Our embedding network is also trained using bi-directional loss, but we carefully explore a number of implementation choices, resulting in a model that can significantly outperform CCA-based methods and scale to large datasets.

Classification-based methods. Learning the similarity between images and text can be also modeled as classification. Deep models can be designed to answer whether two input visual and text samples match each other. For example, Jabri et al. [6] used a softmax function to predict whether the input image and question match with 4 the answer choice for VQA.Rohrbach et al. [7] used a softmax function to estimate the posterior probability of a phrase over all the available region proposals in an image.

Our second network type, the similarity network, also builds on the idea of directly predicting similarity between a phrase and a region through classification. However, instead of softmax loss, we use non-exclusive logistic regression loss and treat each phrase-region pair as an independent binary classification problem – that is, for a given phrase, more than one region in the same image can be positive.

III. EMBEDDING AND SIMILARITY NETWORKS

3.1 Overview of Image-Text Tasks

In this paper, we focus on two image-text tasks: phrase localization and image-sentence retrieval. Phrase localization, also known as text-to-image reference resolution or visual grounding, has recently received lots of attention. Our definition of phrase localization follows: given an image and an entity mention, i.e. noun phrase, taken from a sentence description that goes with that image, the goal is to predict the corresponding bounding box. We solve this task in a retrieval framework: Given the entity mention, we rank a few hundred candidate regions output by a separate region proposal method (e.g., Edge Box) using the similarity score produced by one of our trained networks. Our embedding network computes cosine similarity scores between input phrase and candidate regions in the shared embedding space, while our similarity network directly output similarity scores via regression.

Our second task, bi-directional image-sentence retrieval, refers both to image-to-sentence and sentence-to-image search. The definitions of the two scenarios are straight forward: given an input image, the goal is to find the best matching sentences from a database. Both scenarios are handled identically by nearest neighbor search in the latent image-sentence embedding space. Our embedding network is the most appropriate for this task, as it directly optimizes the bi-directional ranking loss.

3.2 Embedding Network

3.2.1 Network Architecture

The embedding network has two branches, each composed of a series of fully connected (FC) layers, separated by Rectified Linear Unit(ReLU) nonlinearities. The embedding architecture is highly flexible. The two branches can have different numbers of layers. The input scan be either pre-computed features or outputs of other networks (e.g. CNNs or RNNs), and back-propagation of gradients to the input networks is possible. In our work, we focus on investigating the behavior of the two-branch networks and thus stick to pre-computed image and text features, which already give us state-of-the-art results.

3.2.2 Learning Cross-Modal Matching by Ranking

The embedding network is trained using stochastic gradient descent with a margin-based loss that encodes both bi-directional ranking constraints and neighborhood preserving constraints within each modality. This section will discuss the design of our loss function and the strategy of sampling triplets for stochastic gradient descent.

Bi-directional ranking loss. Given a visual input x_i(awhole image or a region), let $Y_i^+$and Y_i^- denote its setsof matching (positive) and non-matching (negative) text samples, respectively. If y_j and $y_k$are positive and negativesamples for x_i, we want the distance between x_i and y_j to be smaller than the distance between x_i and y_k, with a marginofm. This leads to the following triplet-wise constraint.

$$d\left(x_{i},y_j\ \right) + m < d\left(x_{i},y_k\right) \qquad (1)$$

Note that here and in the following, d(x; y) will denote the Euclidean distance between image and text features in the embedding space.

Given a text input $y_{i',}$(a phrase or sentence), we have analogous constraints in the other direction:

$$\mathrm{d}(x_{j'},y_{i'}) + m < d(x_{k'},y_{i'}) \qquad (2)$$

These ranking constraints can be converted into a margin-based loss function:

$$L(X,Y) = \lambda_1 \sum_{i,j,k} [m + d(x_i, y_j) - d(x_i, y_k)]_+$$

$$+\lambda_2 \sum_{i',j',k'} [m + d\left(x_{j'}, y_{i'}\right) - d\left(x_{k'},y_{i'}\right)]$$

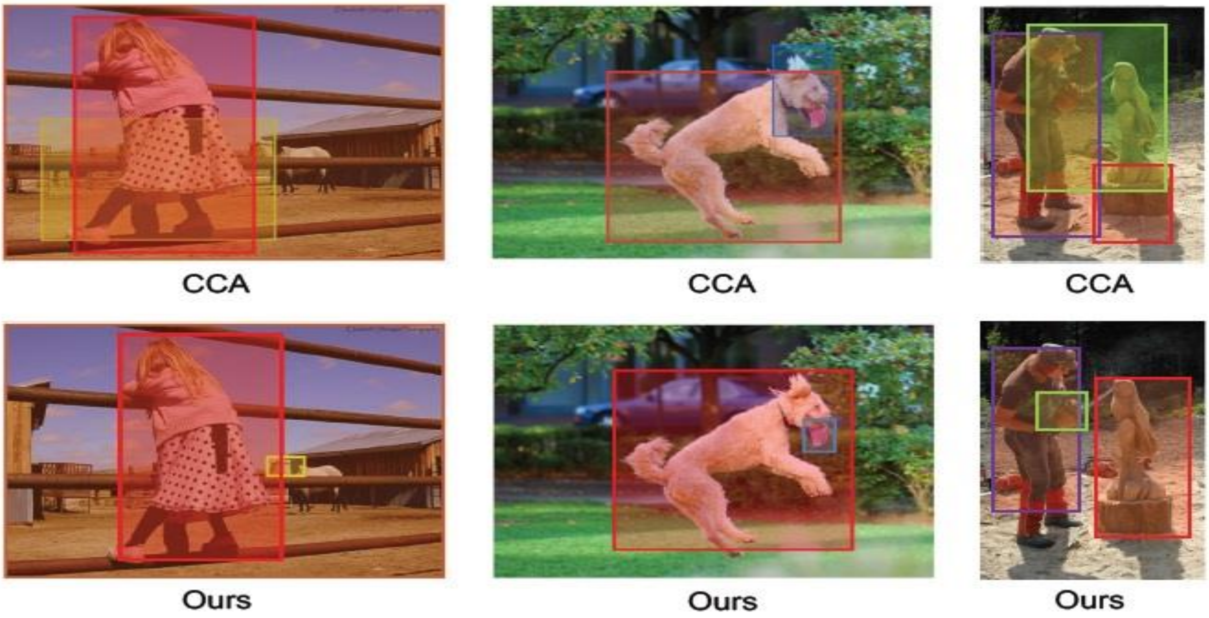
(3)

Our bi-directional ranking loss sums over all triplets (a target instance, a positive match, and a negative match) defined in constraints (1) and (2).For simplicity, we fix the margin m = 0:05 for all terms in our experiments. The weights $\lambda_1$and $\lambda_2$balance the strength ofthe ranking loss in each direction.

IV. PHRASE LOCALIZATION EXPERIMENTS

The phrase localization task was introduced in Section 3.1. To recap briefly, given a query noun phrase from an image caption and a set of region proposals from the same image, we rank the proposals using the region-phrase similarity scores produced by one of our trained networks.

4.1 Training Set Construction



A little girl stands on the fence while peeking through it to look at the horse.

A large yellow dog leaps into the air to catch his Frisbee.

A man is using a chainsaw to carve a wooden sculpture.

In our experience, properly defining positive/negative region-phrase pairs and sampling pairs and triplets of examples during training is crucial for achieving the best performance. Phrase localization is akin to object detection, in that region-phrase scores produced by the embedding should be sensitive not only to semantic correspondence, but also to localization quality, i.e., how much a given region proposal overlaps the ground truth box for a query phrase. By default, given a phrase from a description of a specific image, Flickr30K Entities annotations specify a unique ground truth region.

4.2 Baselines and Comparisons

Our experiments systematically evaluate multiple components of our models, including network structure, sampling of the training set, and different components of the loss function for the embedding network. The full list of variants used in our comparisons is as follows.

Network Architecture. We are interested in how our networks benefit from being able to learn a nonlinear mapping in each branch. For this, we compare two variants:

- **Linear branch structure**: only keeping the first layers in each branch immediately followed by L2normalization.
- **Nonlinear branch structure**: branches consisting of two FC layers with ReLU, batch normalization and L2 normalization.

Selecting Positive Pairs. We evaluate how positive example augmentation contributes to the performance of phrase localization.

Single positive: using the ground truth region for a phrase as the single positive example.

Augmented positive: augmenting ground truth regions with other regions having IoU > 0.7 with it.

4.3 Result Analysis

At test time, we treat phrase localization as the task of retrieving regions matching a query phrase (assumed to be present in the image) from a set of region proposals. For the embedding network, the query phrase and each candidate region are passed through the respective branches to compute their embedded representation, and Euclidean distance (equivalently, cosine similarity) is used as the similarity score. For the similarity network, the score is predicted directly using the logistic formulation. In both cases, we rank regions in decreasing order of similarity to the query and report Recall@K, or the percentage of queries for which the correct match has rank of at most K. A region proposal is considered to be a correct match if it has IoU of at least 0.5 with the ground-truth bounding box for that phrase. Figure 2 shows examples of phrase localization results in three images with our best model (similarity networks with augmented positives) compared to the CCA model.

V. IMAGE-SENTENCE RETRIEVAL

This section evaluates our networks on the task of bidirectional image-sentence retrieval. Given a query image (resp. sentence), the goal is to find corresponding sentences (resp. images) from the dataset. In addition to the Flickr30K dataset, here we perform experiments on the larger MSCOCO dataset, consisting of 123287 images (the combination of released train2014 and val2014 from MSCOCO website) with five sentences each. MSCOCO does not include comprehensive region-phrase correspondence, so we can use it for image sentence retrieval only.

5.1 Baselines and Comparisons

Just as in Section 4, we demonstrate the impact of different components of our models by reporting results for the following variants.

Linear vs. Nonlinear Branch Structure. The same way as in the phrase localization experiments, we want to see the difference made by having one vs. two fully connected layers within each branch.

Embedding Loss Functions. Image-sentence retrieval is a bi-directional retrieval task, so we want to see whether bidirectional loss can give a bigger improvement over the single-directional loss than that on phrase localization task.

❖ **Single-directional**: in Eq.(6), only using the single direction (from image to sentences) by setting λ_1 =1; λ_2 = 0; λ_3 = 0; λ_4 = 0.

❖ **Bi-directional**: in Eq.(6), set λ_1= 1, λ_2 = 1.5, λ_3 = 0, λ_4 = 0. These parameter values are determined on the validation set.

Neighborhood Sampling and Constraints. In bothFlickr30K and MSCOCO datasets, each image is associated with five sentences. we can try to enforce neighborhood structure on the sentence space. We cannot do it on the image space since in the Flickr30K and MSCOCO datasets we do not have direct supervisory information about multiple images that can be described by the same sentence. Thus, in Eq.(6), we always have λ_3= 0.

❖ **Neighborhood sampling**: using the neighborhood sampling strategy (see Section 3.2.3) to replace standard triplet sampling.

❖ **Neighborhood constraints**: using the full loss function as in Eq.(6). This is done by setting λ_2= 1.5, λ_4= 0.05. We always use neighborhood sampling in this case.

5.2 Sentence-to-sentence Retrieval

Our experiments on the embedding network both for phrase localization and image-sentence retrieval have shown that neighborhood sampling can give considerable improvement seven without adding neighborhood constraint terms to the triplet loss. Thus, it is still unclear how neighborhood constraints change the latent embedding space. Therefore, in this section, instead of only looking at cross-modal retrieval, we show how neighborhood constraints can improve performance for the within-view task of sentence-to-sentence retrieval: given a query sentence, retrieve other sentences that correspond to the same image. For the evaluation metric, we still use R@K.

5.3 Combining Image-Sentence and Region-Phrase Models

We have evaluated our networks separately on region-phrase and image-sentence correspondence tasks. The next obvious question is whether the local and global similarity models can be brought together, for example, to improve performance on image-sentence retrieval. Intuitively, it would be nice to have an approach that can verify whether an image and a sentence match based not only on their global features, but on detailed correspondence between regions in the image and phrases in the sentence. Given the high accuracy achieved by our models on phrase localization in Section 4, one would expect that combining it with the image-sentence model of Section 5 would lead to significant improvements. However, one of the most frustrating findings in our work to date is that making such a combination work is highly non-trivial.. Given an image x and a sentence y, we define the combined image-sentence and region-phrase distance as

$$D(x,y) = (1-\alpha)d(x,y) + \alpha\, d_{rp}(x,y), \qquad (7)$$

where $d(x,y)$is the distance in the image-sentence latentspace learned by the embedding network, and $d_{rp}(x,y)$is the average of the distances between all the phrases inthe sentence and their best-matching regions in the image.

The global image-sentence model already works very well for image-sentence retrieval, in that it usually succeeds in retrieving sentences that roughly fit the image. In order to provide an improvement, the region-phrase model would have to make fine distinctions of which it is currently incapable, e.g., between closely related or easily confused objects, between fine-grained attributes of people, or cardinalities of people and objects. Furthermore, due to the way our region-phrase model is trained, its scores are meant to be useful for ranking regions within the same image based on the correspondence to a given phrase that is assumed to be present.

VI. CONCLUSION AND FUTURE WORK

This paper has studied state-of-the-art two-branch network architectures for region-to-phrase and image-to-sentence matching. To our knowledge, our results on Flickr30K and MSCOCO datasets are the best to date on both tasks. Our first architecture, the embedding network, works by explicitly learning a non-linear mapping from input image and text features into a joint latent space in which corresponding image and text features have high similarity. This network works well for both image-sentence and region-phrase tasks, though its objective consists of multiple terms and relies on somewhat costly and intricate triplet sampling. We investigated triplet sampling within mini-batches in detail and showed that the way it is done can have a significant impact on performance, even without changing the objective function. Our second architecture, the similarity network, tries to directly predict whether an input image and text feature are similar or dissimilar. Our experiments showed that this network can serve as an attractive alternative to the embedding network for region-phrase matching, but fails miserably for image-sentence retrieval, revealing an interesting difference between the two tasks. Finally, our preliminary unsuccessful experiments on combining image sentence and region-phrase models indicate an important direction for future research.

REFERENCES

1. Y.Gong, Q. Ke, M. Isard, and S. Lazebnik, "A multi-view embedding space for modeling internet images, tags, and their semantics," *IJCV,* 2014
2. G. Andrew, R. Arora, J. Bilmes, and K. Livescu, "Deep canonical correlation analysis," in ICML, 2013.
3. F. Yan and K. Mikolajczyk, "Deep correlation for matching images and text," in CVPR, 2015.
4. J. Weston, S. Bengio, and N. Usunier, "Wsabie: Scaling up to large vocabulary image annotation," in IJCAI, 2011.
5. A. Frome, G. S. Corrado, J. Shlens, S. Bengio, J. Dean, T. Mikolov et al., "Devise: A deep visual-semantic embedding model," in NIPS, 2013.
6. A. Jabri, A. Joulin, and L. van der Maaten, "Revisiting visual question answering baselines," in ECCV, 2016.
7. A. Rohrbach, M. Rohrbach, R. Hu, T. Darrell, and B. Schiele, "Grounding of textual phrases in images by reconstruction," ECCV, 2016.

Capability-Based Security Enforcement in Named Data Networking

Ms.S.Vanathi
Assistant Professor,
Department of Computer Science and Engineering,
St. Anne's College of Engineering and Technology.

Ms. P.Esther Printina Mary, Ms. A.Kalaiselvi, Ms. M.Manikeerthana.
UG Students
Department of Computer Science and Engineering,
St.Anne's College of Engineering and Technology.

Abstract— Named data networking (NDN) enhances traditional IP networking by supporting in-network content caching for better bandwidth usage and location-independent data accesses for multi-path forwarding. However, NDN also brings new security challenges. For example, an adversary can arbitrarily inject packets to NDN to poison content cache, or access content packets without any restrictions. We propose capability-based security enforcement architecture (CSEA), a capability-based security enforcement architecture that enables data authenticity in NDN in a distributed manner. CSEA leverages capabilities to specify the access rights of forwarded packets. It allows NDN routers to verify the authenticity of forwarded packets, and throttles flooding-based DoS attacks from unsolicited packets. We further develop a lightweight one-time signature scheme for CSEA to ensure the timeliness of packets and support efficient verification. We prototype CSEA on the open-source CCNx platform, and evaluate CSEA via testbed and Planetlab experiments. Our experimental results show that CSEA only incurs around 4% of additional delays in retrieving data packets.

Index Terms— Security, capability, named data networking, MHT algorithm.

I. INTRODUCTION

NAMED Data Networking (NDN) has been proposed to replace the "connection-based" model in traditional IP networking with the "content-based" model. By identifying data packets by names instead of locations, NDN enables flexible in-network caching for improved bandwidth usage and allows location-independent content access for multi-path forwarding . From a security perspective, the name-based transmission model of NDN does not reveal who requests data packets and who hosts data, thereby improving privacy .On the other hand, NDN also brings new security chal-lenges. One key challenge is that authenticity of data packets in NDN cannot be effectively verified by NDN routers since the packets may be from anywhere in the networks . Therefore, an adversary can easily inject faked data packets or replay data packets, so as to poison content cache in NDN networks. In particular, cache poisoning can lead to denial of service (DoS). Also, it is non-trivial to detect and throttle DoS attacks due to the flooding of fake data request packets in NDN. Our key observation is that NDN routers do not have any information about which content providers or users produce data packets. Therefore, NDN routers cannot readily decide if the packets in networks are malicious, although they parse the semantics of packets during packet forwarding.

II. LITERATURE SURVEY

Shapiro et al. develop capability system to enforce resource access control within operating systems. Anderson et al. [3] propose to defend against DoS attacks in IP networks by issuing capabilities for packet sources. In contrast, CSEA targets an NDN system and aims to achieve both data access control and DoS defense through capabilities. Access control enforcement schemes have been proposed for Information Centric Networking (ICN) (of which NDN is an instance).

Fotiou et al. Propose a centralized access control architecture for ICN, in which access control providers issue credentials for data requests. Li et al. propose LIVE, a centralized access control enforcement scheme for NDN. While LIVE also leverages Merkle Hash Trees as CSEA for lightweight data verification, the fundamental difference between LIVE and CSEA is that LIVE enforces access control policies in a centralized manner, while CSEAallows distributed access control. LIVE requires CPs to manage token distribution for access control, and hence routers and users require frequent interactions with CPs to obtain tokens. In contrast, CSEA distributes the load of data verification among NDN routers. Also, CSEA effectivel throttles DoS attacks, which are not considered by LIVE.

2.1. Lightweight integrity verification and content access control for named data networking

Q Li, PPC Lee, P Zhang, P Su, L He… - … on Networking, Named data networking (NDN) enhances traditional IP networking by supporting in-network content caching for better bandwidth usage and location-independent data accesses for multi-path forwarding. However, NDN also brings new security challenges. For example, an adversary can arbitrarily inject packets to NDN to poison content cache, or access content packetswithout any restrictions. We propose capability-based security enforcement architecture (CSEA), a capability-based security enforcement architecture that enables data.

2.2. Anonymous Named Data Networking Application

S. DiBenedetto, P. Gasti, G. Tsudik, and E. Uzun, Content-centric networking — also known as information-centric networking (ICN) — shifts emphasis from hosts and interfaces (as in today's Internet) to data. Named data becomes addressable and routable, while locations that currently store that data become irrelevant to applications.

Named Data Networking (NDN) is a large collaborative research effort that exemplifies the content-centric approach to networking. NDN has some innate privacyfriendly features, such as lack of source and destination addresses on packets. However, as discussed in this paper, NDN architecture prompts some privacy concerns mainly stemming from the semantic richness of names. We examine privacy-relevant characteristics of NDN and present an initial attempt to achieve communication privacy. Specifically, we design an NDN add-on tool, called ANDaNA, that borrows a number of features from Tor. As we demonstrate via experiments, it provides comparable anonymity with lower relative overhead.

III. EXISTING SYSTEM

In existing system propose the lightweight respectability confirmation (LIVE) engineering, an expansion to the NDN convention, to address these two issues. Besides, it permits a substance supplier to control content access in NDN hubs by specifically dispersing uprightness check tokens to approved hubs. We also introduce IP address verification to avoid unauthorized users. Here our tokens valid from the user can access his accounts from another system.

3.1 Drawbacks:

- It cannot be provide token administration for execute CP confirmation amid token refreshment.
- It cannot be fully avoid the attacks.

IV. PROPOSED SYSTEM

In proposed system propose CSEA, a capability-based security enforcement architecture that enables the verification of content authenticity in a distributed manner. CSEA associates each piece of content in NDN with a capability, which can be viewed as a ticket that specifies the access right of the content. In CSEA, capabilities serve two key purposes. First, capabilities enable a CP to authorize content under an access right, similar to the use of capabilities in classical computing systems.

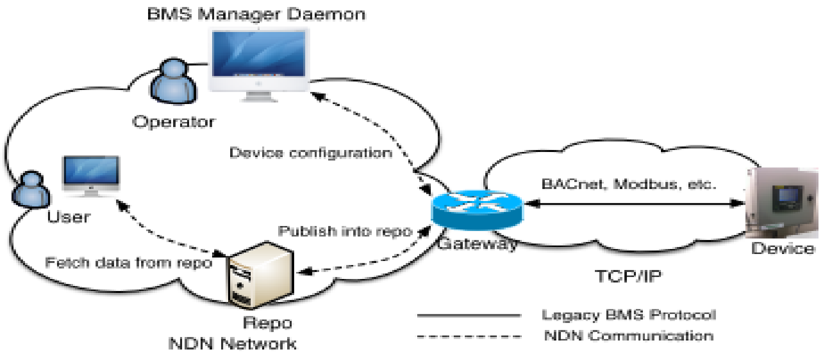


Figure 4.1 Proposed system

Each router includes a capability verifier, which verifies the correctness of capabilities from CPs and tokens from users, and an access control point (ACP*)*, which enforces access control policies and decides whether an interest or data packet should be forwarded or dropped based on the verification results of the capability verifier. The ACP also caches received tokens that are deemed valid, and uses them to verify the subsequently received capabilities and tokens. The lightweight one-time signature scheme for CSEA to ensure the timeliness of packets and support efficient verification. Moreover, it counts and limits the times of valid tokens that are used to request different data packets so as to prevent interesting flooding with valid tokens.

4.1 Advantages:

- It allows NDN routers to verify the authenticity of forwarded packets, and throttles flooding-based DoS attacks from unsolicited packets.
- It ensure timeliness of packets and enable efficient verification of content authenticity.

V. CONCLUSION

In our paper, we proposed CSEA to enforce security policies in NDN such that it can throttle different attacks in NDN, i.e., content poisoning attacks, DoS attacks, and content leakage attacks. Specially, we leverage lightweight hash algorithms to implement a capability system within CSEA. We implemented the CSEA prototype upon the CCNx platform, and demonstrate the benefits of CSEA with testbed and Planetlab experiments. The experimental results show that CSEA introduces negligible overhead in retrieving data packets in NDN.

REFERENCES

1. 1 Q. Li, X. Zhang, Q. Zheng, R. Sandhu, and X. Fu, “LIVE: Lightweight integrity verification and content access control for named data networking,” IEEE Trans. Inf. Forensics Security, vol. 10, no. 2, pp. 308–320, Feb. 2015.
2. S. DiBenedetto, P. Gasti, G. Tsudik, and E. Uzun, “ANDaNA: Anony- mous named data networking application,” in Proc. NDSS, 2012.
3. G. Acs, M. Conti, P. Gasti, C. Ghali, and G. Tsudik, “Cache privacy in named-data networking,” in Proc.ICDCS, Jul. 2013, pp. 41–51.
4. T. Anderson, T. Roscoe, and D. Wetherall, “Preventing Internet denial-of-service with capabilities,” ACM SIGCOMM Comput. Commun. Rev., vol. 34, no. 1, pp. 39–44, 2004.

Human Activity Recognition by Triliteration HMSA

Mrs.M Senthamarai Selvi,
Associate Professor,
Department of Computer Science and Engineering,
St. Anne's College of Engineering and Technology, Panruti.

Mr.R.Rajarajan
Assistant Professor,
Department of Computer Science and Engineering,
St. Anne's College of Engineering and Technology, Panruti.

Ms.Y.Jenifer, Ms.V.Bakkiya
UG Students,
Department of Computer Science and Engineering,
St. Anne's College of Engineering and Technology, Panruti.

Abstract— Elegant strategy such as Smartphone application able to give the functions of a pedometer by the accelerometer. To attain a high correctness the devices contain to be damaged on specific on-body location such as on an armband or in footwear. Usually public carry elegant devices such as Smartphone in different positions, thus making it not practical to use these devices due to the abridged correctness. Using the implanted Smartphone accelerometer in a low-power mode there an algorithm named Energy-efficient Real-time Smartphone Pedometer which accurately and energy-efficiently infers the concurrent person step count within 2 seconds with the Smartphone accelerometer. Technique involves take out 5 features from the Smartphone 3D accelerometer devoid of the need for noise filtering or exact Smartphone on-body placement and compass reading; Energy-efficient Real-time Smartphone Pedometer categorization correctness is around 94% when validated using information collected from 17 volunteers.

Index Terms— Pedometer, Accelerometer, Smartphone, Activity categorization

I. INTRODUCTION

Smart phones provide sophisticated real-time sensor information for dispensation. Researchers contain studied a large number of sensors such as accelerometer, gyroscope, rotation vector, and direction sensors in person step count projects. Of these the accelerometer is the majority precious non-transceiver sensor used to give the information for activity monitoring as it gives more information concerning movement armed forces. Therefore the core center of this system is on using solely the smart phone accelerometer for person pace count. The motivation for MBS, in contrast to LBS, includes:

1. Adapting dynamically the types of mobility information services based upon the travel mode, e.g., a pedestrian map triggered after detecting walking, shows safer places to cross roads whereas a motorist map focuses more on main road routes.
2. Mobility profile driven social and societal behaviour analysis changes via gamification and incentives, e.g., to promote greater low carbon transportation modes and low-energy transport usage.

3. Real-time human mobility profiling, such as determining the degree of physical exercise, the usage patterns for types of public and private transport, low carbon transport usage and the time spent at a location (This latter aspect can indirectly indicate human activities even personal preferences at that location e.g., spending more time near one shop location rather another one can indicate shopping and a greater user preference or interest for one shop as compared to another.
4. Human activity driven system control and optimization, e.g., switching off power hungry location sensors such as the GPS receiver and Wi-Fi when out of range, i.e., when travelling in an underground train.

The accelerometer has three input advantages over transceiver based place signal sensors such as GPS. First, low energy spending of 60 mW. Second, there is no wait when starting the accelerometer, however receiving position updates in GPS depends on the start mode. In a hot start form the Termed-Time-to-Subsequent-Fix is about 10 seconds and in a cold create mode the Time To-First-Fix could take up to 15 minutes. Third, sensors interpretation are incessantly available with the accelerometer as compare to GPS and Wi-Fi which could be thwarted as of signals transmit by GPS satellites and being out of range of Wi-Fi signals in that order. Person movement categorization using smart phones requires a movement condition gratitude technique that can function regardless of the position of the smart phone because placing accelerometers on exact parts of the body makes it not practical for use in the real-world. Acceleration information differs for similar behavior, thus making it harder to finely secernate between certain types of activity. Limits have been found in the range of movement activities identified by use of an only one sensor and; due to the complexity of person movement and noise of sensor signal, action categorization algorithms tend to be probabilistic. They have in its place designed a various modal sensor panel that concurrently captures information from many sensors. A major challenge in the design of ubiquitous, context-aware smart phone applications is the increase of algorithms that can find the person action using noisy and equivocal sensor information. There a technique called Energy-efficient Real-time Smart phone Pedometer; an Android based smart phone application to accurately calculate person steps. The novelty of this investigate as compared to existing systems are: ERSP extracts five features this scheme works an energy-efficient frivolous arithmetical model to process in real-time the activity accelerometer information with no need for noise filtering and works in spite of of the smart phone on-body placement and orientation.

II. RELATED WORK

Takamasa Higuchi, Hirozumi Yamaguchi, and Teruo Higashino proposed a novel social navigation framework, called PCN that leads users to their friends in a crowd of neighbors. PCN provides relative positions of surrounding people based on sensor readings and Bluetooth RSS, both of which can be easily obtained via off-the-shelf mobile phones. Through a field experiment in a real trade fair, demonstrated that PCN improves positioning accuracy by 31% compared to a conventional approach owing to its context-supported error correction mechanism. Furthermore, showed that the geometrical clusters in the estimated positions are highly consistent with actual activity groups, which would help users to easily identify actual nearby people.

Emiliano miluzzo, nicholas d. Lane, kristof fodor, Ronald peterson,mirco musolesi, shane b. Eisenman, xiao heng, hong lu, andrew t. Campbell proposed the execution, evaluation, and user experiences of the CenceMe request, which represents one of the primary application to without human intervention get back and issue sensing attendance to common networks by Nokia N95mobile phones. Described a complete system execution of CenceMe with its presentation assessment. Discussed a number of significant design decisions wanted to resolve various limitations that are there when annoying to deploy an always-on sensing request on a profitable mobile phone. Also obtainable the results from a long-lived experiment where CenceMe was used by 22 users for a three week period. Discussed the user study and lessons learn from the deployment of the request and tinted how might get better the application moving forward.

Jialiu Lin Yi Wang, Murali Annavaram, Quinn A. Jacobson, JasonHong, Bhaskar Krishnamachari,Norman Sadeh, presented the design, execution, and evaluation of an Energy Efficient Mobile Sensing System (EEMSS). The center part of EEMSS is a sensor organization scheme for mobile devices that operates sensors hierarchically, by selectively turning on the minimum set of sensors to monitor user state and triggers new set of sensors if necessary to achieve state transition findion. Energy consumption can be reduced by shutting down unnecessary sensors at any particular time. Implementation of EEMSS was on Nokia N95 devices that use sensor management scheme to manage built-in sensors on the N95, including GPS, Wi-Fi find or accelerometer and microphone in order to achieve person daily activity recognition. Also proposed and implemented novel categorization algorithms for accelerometer and microphone readings that work in real-time and lead to good performance. Finally, we evaluated EEMSS with 10 users from two universities and were able to provide a high level of accuracy for state recognition, acceptable state transition findion latency, as well as more than 75% gain on device lifetime compared to existing system

III. ALGORITHMS

3.1 Movement Categorization Algorithms

Acceleration information also varies for similar activities, thus making it extra difficult to finely differentiate certain type's activity. A major challenge in the design of ubiquitous, context-aware smart phone applications is the growth algorithms that can find the person movement state using noisy and equivocal sensor information. Limits have been found in the range of movement activities recognized by use of single sensor mainly and; due to the difficulty of person movement and noise of sensor signals, movement categorization algorithms tend to be probabilistic.

3.2. Accelerometer Based Algorithm

This algorithm works an energy-efficient light-weight exact model to process in real-time the movement accelerometer information without the need for noise filtering and it works regardless of the smart phone on-body placement and compass reading. This method adapts the standard Support Vector Machine (SVM) and exploits fixed-point arithmetic for computational cost reduction. In terms of person movement analysis, our accelerometer based algorithm can be used separately or as part of mixture structural design, e.g., it can be used in a joint accelerometer and location strength of mind approach.

3.3. Different Person Movement Patterns Tend To Be Generated Algorithms

The algorithm have to be able to adapt to the various variation as a user is performing an activity, e.g., what is classified as walking for a sure group might be confidential as jogging for another group. The first step involves personalizing EHMS by reconfiguring the algorithm based on the smart phone accelerometer information gathered for the exact activity. A comparison with the traditional SVM shows a significant improvement in terms of computational costs while maintaining similar accuracy, which can contribute to develop more sustainable systems for Ambient Intelligence. To personalize the application based on a specific action, the user performs the activity for a one-off time of 14 seconds. Fourteen seconds was chosen because a minimum of 56 accelerometer samples are required to cover the T range from 0 to 6.

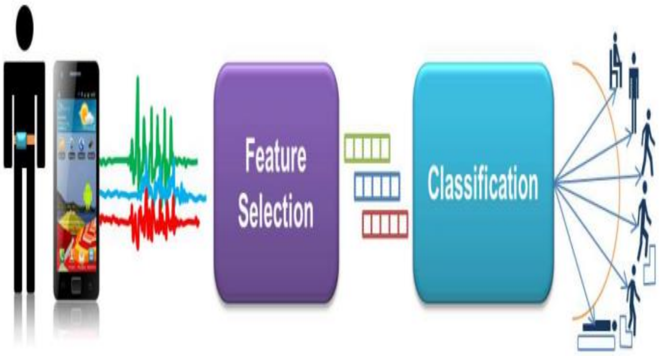


Figure 3.1-Accelerometer Noise Filtering

The Kalman filter outstanding the algorithm's aptitude to efficiently computes accurate estimate of the true value given noisy capacity. The accelerometer readings give sensibly precise information for movement findion, and for this cause the Kalman filter algorithm is well suited for filtering the Gaussian process and to aid in real-time person movement state calculation. Also there is no need to retain historical measurements and estimates as only the present and self-assurance estimate levels are required. From the unprocessed information the same feature, extracted intended for categorization. It takes less memory. To personalize the application based on a specific action, the user performs the activity for a one-off time of 14 seconds.

IV. RESULTS

The experiments conducted involved the study of accelerometer data gathered from various activities. The key objective of the scientific experiment is to investigate features such as peaks and troughs that can be extracted from the accelerometer readings to classify similar human mobility states such as travel by light rail train vs. underground train. The data collection process was conducted by 15 participants for 12 different activities. In order to validate EHMS we required a wide range of realistic user data to stress test the algorithm. The activities were selected because they were amongst the most popular types of modality and offered a wide range of normal urban commuting activities. Table 2 shows the activities recorded by each user. EHMS uses aggregated classes for user activity classification, e.g., although users 12 and 13 only performed two activities, their samples are classified using the aggregated class (which has all 12 types of activities). Users 1 to 13 were permitted to carry the smartphone regardless of the on-body placement. Users 14 and 15 had to place the smartphone in predetermined body positions. This allowed us to study the differences in accelerometer readings based upon different smartphone on-body placements and orientations. For each activity we used 1,250 training data points. This is equivalent to 312.5 seconds per activity. We chose 1,250 samples because the data gathering process required each participant to perform an activity for a minimum of 360 seconds. It should be noted that we found 14 seconds (56 samples) was sufficiently long to personalize the EHMS Android application for a specific user activity. In this paper real world data was gathered using Android based smartphones. No accelerometer data noise filtering or data simulation was used. In several cases even similar activities cannot be grouped together, e.g., it can be argued that different kinds of low and high speed over ground trains will generate different human mobility profiles. We selected a small subset of human mobility states for demonstration purposes since EHMS can be dynamically applied to a wide range of human mobility states. 4.1 Accelerometer Noise Filtering For optimum classification accuracy, a comparatively low sampling frequency of 4 Hz is used by EHMS and the window size for feature extraction is 2 seconds. If the frequency isn't 4 Hz then EHMS still uses eight accelerometer samples per cycle for classification, but will misclassify activities since the window size is no longer 2 seconds. The Kalman filter is a parametric model that can be applied to both stationary and in-motion human mobility data analysis [24]. We investigated whether or not a discrete Kalman filter algorithm could filter the accelerometer noise thus ameliorating the activity state detection accuracy estimation. We chose to use the Kalman filter due the algorithm's ability to efficiently compute accurate estimates of the true value given noisy measurements. The accelerometer readings provide reasonably accurate data for mobility detection, and for this reason the Kalman filter algorithm is well suited for filtering the Gaussian process and to aid in real-time human mobility state prediction. Also there is no need to retain historical measurements and estimates as only the current and confidence estimate levels are required.

V. ANALYSIS

Evaluated EHMS using existing classifiers. The classifiers are J48, decision table (DT), bagging, and naive bayes. Fig. shows the precision and remembers contrast of EHMS vs. known existing classifiers with and without personalization.

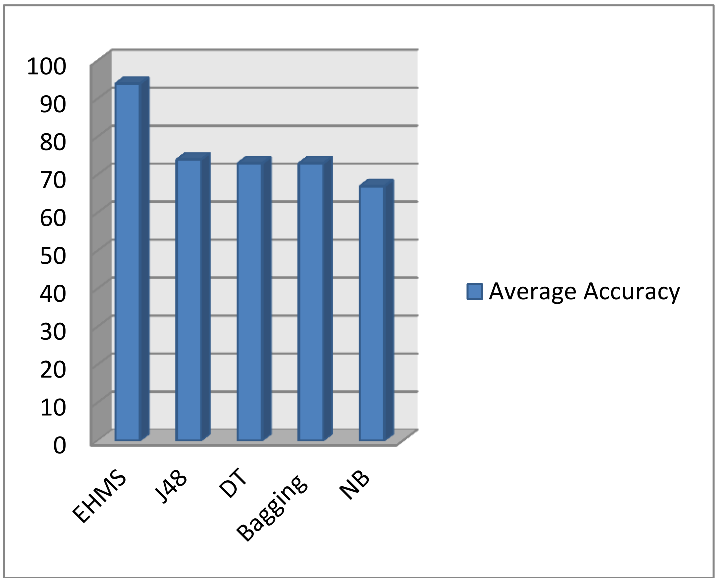


Fig.1 EHMS vs. known existing classifiers

Trained the classifiers using an information set comprised of pre-classified accelerometer information for the following activities: light rail train, car, jogging, lying down, stationary and walking. To obtain a model for the classifiers, the classifiers were trained using the same set of 1,250 accelerometer samples for every action with a 10 fold cross-validation. From the unprocessed information the same feature, extracted intended for categorization. It takes less memory. Contrast with other existing classifier EHMS is makes the better accuracy it shown in below chart.

VI. CONCLUSION

Concurrent person movement state categorization algorithm without need for referencing historical information. Categorization of the person movement state regardless of the smart phone position and on-body placement. The proposed representation is comparatively insensitive to noisy information. Found even though the noise was reduced when Kalman filtering was applied, the computational features were stymied in the output making it use superfluous in classifying between different person movement conditions. Light-weight accelerometer information feature extraction. EHMS extracts five novel features counting one derived feature from the accelerometer information. Further there is no need for a remote server link for computational purposes as all processing is performed inside the smart phone. More energy-efficiency due to the small computational algorithms and smart phone implanted accelerometer sensing mode at four samples per instant.

REFERENCES

1. V. Devadas and H. Aydin, "On the interplay of voltage/frequency scaling and device power management for frame-based real-time embedded applications," IEEE Trans. Comput., vol. 61, no. 1, pp. 31–44, Jan. 2012.
2. I. Constandache, S. Gaonkar, M. Sayler, R. R. Choudhury, and L. Cox,"EnLoc: Energy-efficient localization for mobile phones," in Proc. 28th IEEE Int. Conf. Comput. Commun., 2009, pp. 2716–2720.
3. F. A. Levinzon, "Fundamental noise limit of piezoelectric accelerometer," IEEE Sensors J., vol. 4, no. 1, pp. 108–111, Feb. 2004.
4. T. Choudhury, G. Borriello, S. Consolvo, B. Harrison, J. Hightower, A. LaMarca, L. LeGrand, A. Rahimi, A. Rea, B. Hemingway, P. Klasnja, K. Koscher, J. A. Landay, J. Lester, D. Wyatt, and D. Haehnel, "The mobile sensing platform: An embedded activity recognition system," IEEE Pervasive Comput., vol. 7, no. 2, pp. 32–41, Apr.–Jun. 2008.
5. H. Zeng and M. D. Natale, "An efficient formulation of the realtime feasibility region for design optimization," IEEE Trans. Comput., vol. 62, no. 4, pp. 644–661, Apr. 2013.

Web-Based Automated Timetable Scheduling

Ms. K. Ezhilarasi, Ms. V. Parkavi
UG Students,
Department of Computer Science & Engineering
C.K College of Engineering & Technology.

Abstract - The hand operated system of time table preparation in our colleges is very monotonous and time-consuming which results in either the same teachers ending up with more than one class at a time or a number of classes conflicting at the same classroom. Due to a non-automatic perspective, absolute utilization of resources has proven ineffective. The automatic time table scheduling provides easier ways for teachers and students to view their timetable once the Admin are finalized over the Web-application having individual login id and password. Our project introduces a practical automated timetabling approach for our college to overcome the hand operated system and conflicts occur in existing system using genetic algorithm(GA). Here we also introduce a dynamic attribute for new announcement such as seminar and special classes.

***Index Terms - GA, Population*.**

I. INTRODUCTION

Our college has a number of different courses and each course has a number of subjects. Now there are limited faculties, each faculty teaching more than one subjects. So now the time table needed to schedule the faculty at provided time slots in such a way that their timings do not overlap and the time table schedule makes best use of all faculty subject demands. We use a genetic algorithm for this purpose. In our Timetable Generation algorithm we propose to a timetable object. This object comprises of Classroom objects and the timetable for every them likewise a fitness score for the timetable. Fitness score relates to the quantity of crashes the timetable has regarding alternate timetable for different classes. Classroom object comprises of week objects. Week objects comprise of Days, Days comprises of Timeslots. Timeslot has an address in which a subject, student gathering going to the address and educator showing the subject is related. Also, further on discussing the imperatives. We have utilized composite configuration design, which make it well extendable to include or uproot as numerous obligations. In every obligation class the condition as determined in our inquiry is now checked between two timetable objects. On the off chance that condition is fulfilled i.e. there is a crash is available then the score is augmented by one.

II. LITERATURE SURVEY

Genetic algorithms are general search and optimization algorithms inspired by processes and normally associated with natural world. Genetic algorithm mimics the process of natural selection and can be used as a technique for solving complex optimization problems. Genetic algorithms are methods of solving problems based upon an abstraction of the process of Natural Selection. They attempt to mimic nature by evolving solutions to problems rather than designing them. Genetic algorithms work by analogy with Natural Selection as follows. First, a population pool of chromosomes is maintained. The chromosomes are strings of symbols or numbers. There is good precedence for this since humans are defined in DNA using a four-symbol alphabet. The chromosomes are also called the genotype (the coding of the solution), as opposed to the phenotype (the solution itself). In the Genetic algorithm, a pool of chromosomes is maintained, which are strings. These chromosomes must be evaluated for fitness. Poor solutions are purged and small changes are made to existing solutions and then allow "natural selection" to take its course, evolving the gene pool so that steadily better solutions are discovered. The basic outline of a Genetic Algorithm is as follows: [5] Initialize pool randomly *For each generation { Select good solutions to breed new population Create new solutions from parents Evaluate new solutions for fitness Replace old population with new ones }* The randomly assigned initial pool is presumably pretty poor. However, successive generations improve, for a number of reasons:

1. **Chromosome representation:** Chromosome is a set of parameters which define a present solution to the problem that the genetic algorithm is trying to solve. The chromosome is often represented as a simple string. The fitness of a chromosome depends upon how well that chromosome solves the problem at hand.

```
Create a population of creatures.
Evaluate the fitness of each creature.
While the population is not fit enough:
        {
            Kill all relatively unfit creatures.
            While population size< max;
            {
                Select two population members.
                Combine their genetic material to create a new creature.
                Cause a few random mutations on the new creature.
                Evaluate the new creature and place it in the population.
```

2. **Selection:** During each successive generation, a proportion of the existing population is selected to breed a new generation. Individual solutions are selected through a fitness-based process, where fitter solutions (as measured by a fitness function) are typically more likely to be selected.

3. **Mutation**: It allow the algorithm to avoid local minima by preventing the population of chromosomes from becoming too similar to each other, thus slowing or even stopping evolution.

```
for each gene individual {
 if(p$^{(Random)}$< pm){
gene = get random value from possible values list;
                        }
                }
```

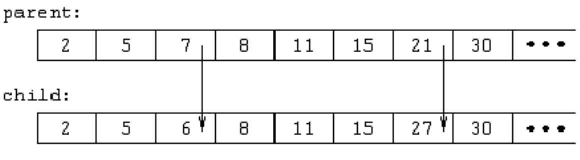


Figure 1: Mutation for Individual [1]

4. **Crossover**: It combines the genetic material from parents order to produce children, during breeding. Since only the good solutions are picked for breeding, during the selection procedure, the crossover operator mixes the genetic material, in order to produce children with even greater fitness. *Crossover Individual.*

For example, assume single point crossover at position 3 two binary chromosomes with values (000000, 111111) will produce (000111, 111000) as children. Moreover, there can be multiple point crossover. What propose here, is an "automatic" way of selecting the best action to execute upon an event occurring? The action is selected by a genetic algorithm. For the moment conditions are supported by active rules when an event has occurred the system can take several actions. For each of possible events, the system holds an ordered set of possible actions that can be taken when the event occurs. The first action is always selected, but a genetic algorithm running in parallel may dynamically change the order of the actions.

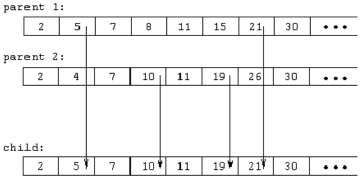
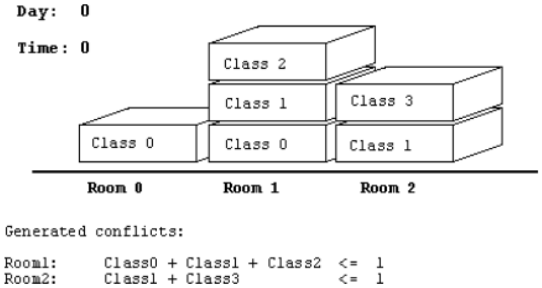


Figure 2: Crossover Individual [1]

Since the genetic algorithm controls the way the agents (constraints) respond to events, the reactive behavior of the agent is controlled by the genetic algorithm. But there can also be another "level" (the "rational" level) to control the agent, especially if an architecture is part of an agent built partially using another method and controlled partially by the constructs this method provides. Actions will be selected for execution using the traditional approach, but some others using the GA approach. This rational part of the agent can also control several parameters of the GA, restart it when needed, or schedule it to be run. This architecture can also be embedded in more complex systems. When an event/action language is necessary for the building of an agent type system, this method can be used for a subset of the events and the actions of the system. This simplifies the design and reduces testing and maintenance times when compared to a deterministic ruleset with many conditions and checks.



```
Generated conflicts:

Rooml:     Class0 + Classl + Class2  <=  1
Room2:     Classl + Class3           <=  1
```

Figure 3: Generation of conflicts and bounds

III. EXISTING SYSTEM

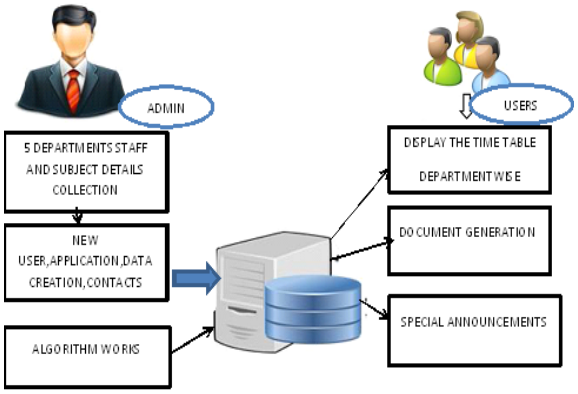
In existing system, our college utilized practical hand operated system for 5 department timetable scheduling. It is very time consuming and tedious to timeslot the faculty in each department without conflict. Each department varies with subjects but some syllabuses are same for the other department. Particular subject handling faculty is needed for both departments, since conflict does not occur in existing system but work delays. In case of special announcement, sometimes it is not conveyed to all students.

IV. PROPOSED SYSTEM

To overcome the practical difficulties that are faced by our faculties and to reduce the time spend for allocating time table for departments, we have proposed automatic timetable Scheduling. Since the available automated time table generators does not satisfies the constraints that are required by our college. We here proposed the system to satisfy our college constraints and to minimize the difficulties for generating time table by our faculties. The present system has „L‟‟ no of lecturers, „S‟‟ no of subjects and „C‟ no of classes per subject in a week. Each day has „H‟ no of hours and we have six working days per week. The total no of time slots then become equal to 6*H. The problem then becomes assigning Subjects for corresponding classes in the 6*H‟ time slots. For example in the department of Computer Science and Engineering, there are n lecturers allotted by admin based on credit for each subject and 6*3 subjects for all the classes per week giving a total number of 3S*n classes per week for three classes. Each day has n hours and six days per week giving n*S time slots for a class. See Table 1 has sample subjects allotted.

Rahul	C #, CN,
Simran	DS,JAVA
Rashmi	C++,HTML
Santhosh	DBMS,CNS

In order to check it is necessary to store sufficient detail about the departments. This means that information concerning all lecturers, classrooms and classes must be maintained. The set of all lecturers is stored as an array. Similarly, there are arrays of lectures and of classrooms. Each of these elements is identified uniquely by its position in the relevant array. The set of all information concerning lecturers, lectures and classrooms are necessary data.


ADMIN
USERS
5 DEPARTMENTS STAFF AND SUBJECT DETAILS COLLECTION
NEW USER,APPLICATION,DATA CREATION,CONTACTS
ALGORITHM WORKS
DISPLAY THE TIME TABLE DEPARTMENTWISE
DOCUMENT GENERATION
SPECIAL ANNOUNCEMENTS

4.1. Advantages

- Faculty did not need to worry for time clashes.

- Authority now does not need to perform permutation and combination
- Authority can concentrate on other things rather than wasting their time on preparing Time-Table

V. CONCLUSION

Timetable generation application will simplify the process of time table generation which may otherwise needed to done using spread sheet manually possibly leading to constraints problem that are difficult to determine when timetable is generated manually. The intention of the system is to generate the time table automatically.

REFERENCES

1. Solving Timetable Scheduling Problem by Using Genetic Algorithms Branimir Sigl, Marin Golub, Vedran Mornar Faculty of Electrical Engineering and Computing, University of Zagreb Unska 3, 10000 Zagreb, Croatia.
2. D. G. Maere, (2010). "How Working Group Automated Timetabling was founded", retrieved from http://www.asap.ac.nott.ac.uk/, 2010, Last accessed date 9th December 2011.
3. J .J. Moreira, "A System for Automatic Construction for Examination Timetable Using Genetic Algorithm".The Techne Polytechnic Studies Review Journal, Vol.6 No.9 2008.
4. Manisha P. Pai, Anirudha Nanda, andAbhijeetGole,"An Algorithm to Automatically Generate
5. Schedule for School Lectures Using a Heuristic Approach",International Journal of Machine Learning and Computing, August 2012.
6. Sanjay R. Sutar , Rajan S. Bichkar"university timetabling hard constraints based technique using genetic algorithm"

Privacy Preservation Scheme of Face Identification with Multiparty Access in Net Banking Environments

Ms. K.Abirami, Ms. K.Dhivya, Ms. K.Karpagam
UG Students
Department of Computer Science and Engineering,
MRK Institute of Technology, Kattumannarkoil.

,

Abstract - The providers of Internet banking services must be more responsive towards security requirements. Now a days with the network world, the way for cybercrime is become easier for hacking purpose. Because of this reason, network security has become one of the biggest facing today's IT departments security. While there is no doubt that Internet banking transaction should have layered protection against security threats, the providers should approach security considerations as part of their service offerings. And heard a lot about hackers and crackers ways to steal any logical password or pin code number character, crimes of ID cards or credit cards fraud or security breaches. In existing framework, Identification can be equated to a username and is used to authorize access to a system. As usernames can be lost or stolen, it is necessary to validate that the intended user is really the person he or she claims to be – the authentication process. Biometric based authentication and identification systems are the new solutions to address the issues of security and privacy. The Face Recognition is the study of physical or behavioral characteristics of human being used for the identification of person. These physical characteristics of a person include the various features like fingerprints, face, hand geometry, voice, and iris biometric device. So implement real time authentication system using face biometrics for authorized the person for online banking system. The general objective of the paper is to develop fully functional face recognition, verification system provide and understand the key aspects of these major technologies, namely those relating to the technological, application entity domain, social environmental system and performance aspects. And also provide multiparty access system to allow the multiple persons to access the same accounts by providing access privileges to original account holders. Experimental results show that the proposed system provide high level security in online transaction system than the existing traditional cryptography approach.

Index Terms - Internet banking, Face biometrics, Authentication system, Multi party access

I. INTRODUCTION

Biometrics refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. Biometric identifiers are then distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice. Some researchers have coined the term behavior-metrics to describe the latter class of biometrics. Fig 1 shows the block diagram illustrates the two basic modes of a biometric system. First, in verification (or authentication) mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be.

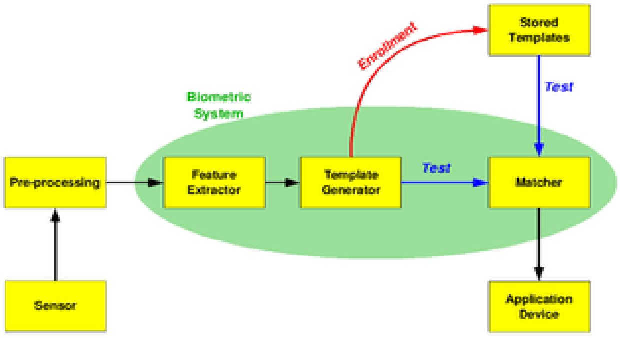


Fig 1: Block diagram of biometric system

Three steps are involved in the verification of a person. In the first step, reference models for all the users are generated and stored in the model database. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. Third step is the testing step. This process may use a smart card, username or ID number (e.g. PIN) to indicate which template should be used for comparison. 'Positive recognition' is a common use of the verification mode, "where the aim is to prevent multiple people from using the same identity".

Second, in identification mode the system performs a one-to-many comparison against a biometric database in an attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be". The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective.

The first time an individual uses a biometric system is called enrollment. During the enrollment, biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block necessary features are extracted. This step is an important step as the correct features need to be extracted in the optimal way.

During the enrollment phase, the template is simply stored somewhere (on a card or within a database or both). During the matching phase, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area). Selection of biometrics in any practical application depending upon the characteristic measurements and user requirements. In selecting a particular biometric, factors to consider include, performance, social acceptability, ease of circumvention and/or spoofing, robustness, population coverage, size of equipment needed and identity theft deterrence. Selection of a biometric based on user requirements considers sensor and device availability, computational time and reliability, cost, sensor size and power consumption

1.1 Multimodal biometric:

Multimodal biometric systems use multiple sensors or biometrics to overcome the limitations of unimodal biometric systems. For instance iris recognition systems can be compromised by aging irises and finger scanning systems by worn-out or cut fingerprints. While unimodal biometric systems are limited by the integrity of their identifier, it is unlikely that several unimodal systems will suffer from identical limitations. Multimodal biometric systems can obtain sets of information from the same marker (i.e., multiple images of an iris, or scans of the same finger) or information from different biometrics (requiring fingerprint scans and, using voice recognition, a spoken pass-code).

Multimodal biometric systems can fuse these unimodal systems sequentially, simultaneously, a combination thereof, or in series, which refer to sequential, parallel, hierarchical and serial integration modes, respectively. Fusion of the biometrics information can occur at different stages of a recognition system. In case of feature level fusion, the data itself or the features extracted from multiple biometrics are fused. Matching-score level fusion consolidates the scores generated by multiple classifiers pertaining to different modalities. Finally, in case of decision level fusion the final results of multiple classifiers are combined via techniques such as majority voting.

II. RELATED WORK

Luigi Atzori, et.al,…[1] a novel paradigm that is rapidly gaining ground in the scenario of modern wireless telecommunications. The basic idea of this concept is the pervasive presence around us of a variety of things or objects – such as Radio-Frequency IDentification (RFID) tags, sensors, actuators, mobile phones, etc. – which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals. Actually, many challenging issues still need to be addressed and both technological as well as social knots have to be untied before the IoT idea being widely accepted.

Shanzhi Chen, et.al,…[2] implemented a technology and economic wave in the global information industry after the Internet. The IoT is an intelligent network which connects all things to the Internet for the purpose of exchanging information and communicating through the information sensing devices in accordance with agreed protocols. It achieves the goal of intelligent identifying, locating, tracking, monitoring, and managing things. It is an extension and expansion of Internet-based network, which expands the communication from human and human to human and things or things and things. In the IoT paradigm, many objects surrounding us will be connected into networks in one form or another. RF identification (RFID), sensor technology, and other smart technologies will be embedded into a variety of applications. Using RFID, sensors, and two-dimensional barcode to obtain the object information at anytime and anywhere, it will be a new opportunity

Huansheng Ning, et.al,…[3] analyzed paradigm to realize universal interactions among the ubiquitous things through heterogeneous spaces. The future IoT is expected to be characterized by the comprehensive perception, reliable transmission, and intelligent processing to achieve pervasive interconnections, intelligence, and efficiency. It enables things to establish dynamical and seamless interconnections across heterogeneous spaces. During the things' interactions, it brings out a series of explosions of connection, information, service, and intelligence. Smart connectivity and effective interactions for addressing a certain task with an ultimate performance are highly demandin trends.

Tie Qiu,et.al,…[4] provide peer to peer networks and each node has functions of data collecting, storage, processing and forwarding. It is the cost-effective solution for the short-range communication in some particular scenarios, such as battlefield, disaster rescue, environment sensing, etc. In order to improve the Quality of Service (QoS) among different heterogeneous network units, HANETs become the research focus in recent years. HANETs usually consist of wireless sensor networks (WSNs), smart ad hoc networks, wireless fidelity networks, telecommunication networks, vehicular ad hoc networks (VANETs), etc.

Jianhua Ma, et.al,..[5] designed an efficient TRE solution for services that are deployed in the cloud and dominated by the data transfer from the cloud servers to the clients. We propose a Cooperative end-to-end TRE solution, named as CoRE, with capability of removing both short-term and long-term redundancy such that traffic redundancy can be eliminated to the highest degree. CoRE involves two layers of cooperative TRE operations. The first-layer TRE performs prediction-based Chunk-Match similar to PACK to capture long-term traffic redundancy. The second-layer TRE identifies maximal duplicate substrings within an outgoing chunk compared with the previously transmitted chunks in a local chunk cache at the sender, referred to as In-Chunk Max-Match.

III. EXISTING METHODOLOGIES

Online security remains a challenge to ensure safe transacting on the internet. User authentication, a human-centric process, is regarded as the basis of computer security and hence secure access to online banking services. The increased use of technology to enforce additional actions has the ability to improve the quality of authentication and hence online security, but often at the expense of usability. Today, there are a number of technologies in use to combat fraud in the banking industry. One of these is the use of One Time Passwords (OTPs), which is a fraud prevention technology specific for e-banking transactions. The most basic method displays a time-dependent code that a user is required to input into the banking interface. Smart cards and USB tokens are other security measures employed by banks that work by verifying the user through their possession of a smart card or USB device. The problem is that all existing security measures present one challenge or the other. Transaction monitoring is a different type of approach that comes from an adaptation of credit/debit card fraud prevention systems. This approach analysis the sender and receiver of the transaction and compares with identified fraud patterns. Any similarity results in the transaction being declined or transferred to a call center for manual verification. This approach requires no additional hardware for the user as all analysis is done in the background. However, this too comes with its disadvantages, as there will be a loophole in the system when new fraud patterns occur before they are detected. Also, occasionally genuine transactions will be forwarded to call centers which then inconvenience customers

IV. PROPOSED METHODOLOGIES

Online banking is now very popular among consumers because it provides a convenient way to perform transactions from anywhere using smart devices. Now a days thieves are using high tech methods to gain access to user information such as passwords, PINs and security questions. This project aims at enhancing the security of Internet banking system with additional face biometric Authentication combination. Internet banking now uses Static User ids and passwords along with OTP-One time Passwords to mobile number. Although this is the best security feature available to date, this security method is still vulnerable and it is very important to enhance the existing security. The term biometrics refers to the emerging field of technology devoted to the identification of individuals using biological behaviors. Biometrics is a powerful combination of science and technology that can be used to protect and secure our most valuable information. Biometrics is not into

Internet banking applications yet. It is because of the practical difficulties and it is very expensive to implement and execute this technology. But, now with technology advancement and cost of Biometric devices coming down, we have probabilities to integrate Biometric Technology to Online Banking. Face biometric can be used to provide cost effective rather than other biometric features such as fingerprint, iris and other features. And also extend the process to implement the system with multiparty access. The user of the account is considered as primary user. The primary user provides the permission to access account to other persons considered as secondary users. The primary user set the limit for secondary access. At the time of login verification, face can be recognized as whether it is primary or secondary. The OTP based password can be send at the time transactions. Finally SMS alert send to primary user with detail description of user name, time of access, amount details. Session time analysis can be used prevent from infrequent access.

4.1 Iterative Closest Point Algorithm:

In The Iterative Closest Point or, in some sources, the Iterative Corresponding Point, one point cloud (vertex cloud), the reference, or target, is kept fixed, while the other one, the source, is transformed to best match the reference. The algorithm iteratively revises the transformation (combination of translation and rotation) needed to minimize an error metric, usually the distance from the source to the reference point cloud. ICP is one of the widely used algorithms in aligning three dimensional models given an initial guess of the rigid body transformation required. Given 2 points r_1 and r_2 , the Euclidean distance is:

Given a point r_1 and set of points A , the Euclidean distance is:

$$d(r_1, r_2) = \|r_1 - r_2\| = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2}$$

The sceneshape S is aligned to be in the best alignment with the model shape M.

$$d(r_1, A) = \min_{i \in 1..n} d(r_1, a_i)$$

The distance of each point s of the scene from the model is:

$$d(s, M) = \min_{m \in M} d\|m - s\|$$

Algorithm steps as follows:

```
function ICP(Scene,Model)
begin
        E` ← + ∞;
        (Rot,Trans) ← In Initialize-Alignment(Scene,Model);
        repeat
                E ←E`;
                Aligned-Scene ← Apply-Alignment(Scene,Rot,Trans);
                Pairs ← Return-Closest-Pairs(Aligned-Scene,Model);
                (Rot,Trans,E`)←Update-Alignment(Scene,Model,Pairs,Rot,Trans);
        Until |E`- E|  < Threshold
        return (Rot,Trans);
end
```

4.2 KNN classifier:

In face recognition, the KNN algorithm is a method for classifying objects based on closest training examples in the feature space. KNN is a type of instance-based learning, or lazy learning where the function is only approximated locally and all computation is deferred until classification. The KNN is the fundamental and simplest classification technique when there is little or no prior knowledge about the distribution of the data. This rule simply retains the entire training set during learning and assigns to each query a class represented by the majority label of its k-nearest neighbors in the training set. The Nearest Neighbor rule (NN) is the simplest form of KNN when K = 1. In this method each sample should be classified similarly to its surrounding samples. Therefore, if the classification of a sample is unknown, then it could be predicted by considering the classification of its nearest neighbor samples. Given an unknown sample and a training set, all the distances between the unknown sample and all the samples in the training set can be computed. The distance with the smallest value corresponds to the sample in the training set closest to the unknown sample. Therefore, the unknown sample may be classified based on the classification of this nearest neighbor. The algorithm steps as follows:

```
for all the unknown samples UnSample(i)
    for all the known samples Sample(j)
        compute the distance between
        Unsamples(i) and Sample(j)
    end for
    find the k smallest distances
    locate the corresponding samples
    Sample(j1),….,Sample(jK)
    assignUnSample(i) to the class which appears more frequently
end for
```

The performance of a KNN classifier is primarily determined by the choice of K as well as the distance metric applied. The estimate is affected by the sensitivity of the selection of the neighborhood size K, because the radius of the local region is determined by the distance of the Kth nearest neighbor to the query and different K yields different conditional class probabilities. The proposed work is shown in fig 2.

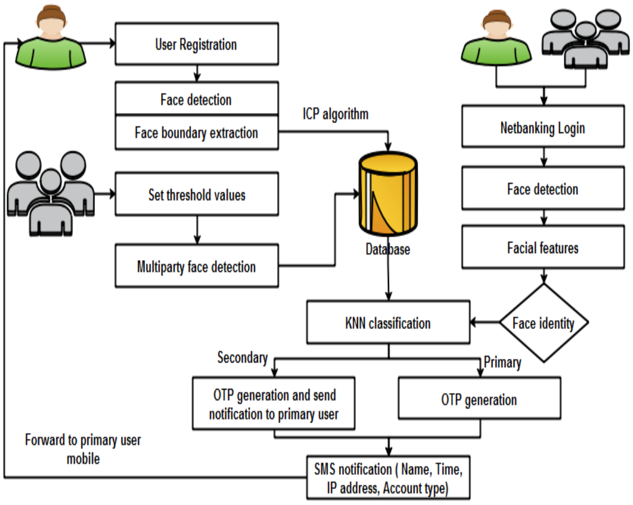


Fig 4.1. Proposed Framework

V. CONCLUSION

As the level of security breaches and transaction frauds increase day by day, the need for highly secure identification and personal verification information systems is becoming extremely important especially in the banking and finance sector. In this paper, we can implement face recognition system to online net-banking application in IOT environments. Face Recognition features can be used to make net-banking systems more secure for authentication purpose in banking based security systems. The ID can be stolen; passwords can be forgotten or cracked but the physical characteristics of a person cannot be stolen or hacked. The Face Recognition identification overcomes all the above. And also provide multi-person access control to provide access privileges to users with improved security. Real time alert system about unauthorized access and multi person access.

REFERENCES

1. L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” Computer networks, vol. 54, no. 15, pp. 2787-2805, 2010.
2. S. Chen, H. Xu, D. Liu, and B. Hu, “A Vision of IoT: Applications, Challenges, and Opportunities WithChina Perspective,” IEEE Internet of Things Journal, vol. 1, no. 4, pp. 349-359, 2014.
3. H. Ning, H. Liu, J. Ma, L. T. Yang, and R. Huang, “Cybermatics:Cyberphysical-social-thinking hyperspace based science and technology,” Future Generation Computer Systems, vol. 56, pp. 504-522, 2016.
4. T. Qiu, N. Chen, K. Li, D. Qiao, and Z. Fu, “Heterogeneous ad hoc networks: Architectures, advances and challenges,” Ad Hoc Networks, vol. 55, pp. 143-152, 2017.
5. H. Song, R. Srinivasan, T. Sookoor, and S. Jeschke, Smart Cities: Foundations, Principles and Applications. Hoboken, NJ, USA: Wiley, 2017.
6. J. Ma, J. Wen, R. Huang, and B. Huang, “Cyber-Individual Meets Brain Informatics,” IEEE Intelligent Systems, vol. 26, no. 5, pp. 30-37, 2011.
7. J. Miranda, N. Makitalo, J. Garciaalonso, J. Berrocal, T. Mikkonen, C. Canal, et al., “From the Internet of Things to the Internet of People,” IEEE Internet Computing, vol. 19, no. 2, pp. 40-47, 2015.
8. H. Ning and H. Liu, “Cyber-physical-social-thinking space based science and technology framework for the Internet of Things,” Science China Information Sciences, vol. 58, no. 3, pp. 1-19, 2015.
9. D. L. Brock, “The electronic product code (epc),” Auto-ID Center White Paper MIT-AUTOID-WH-002, 2001.
10. N. Koshizuka and K. Sakamura, “Ubiquitous ID: standards for ubiquitous computing and the Internet of Things,” IEEE Pervasive Computing, vol. 9, no. 4, pp. 98-101, 2010.
11. H. Ning, S. Hu, W. He, Q. Xu, H. Liu, and W. Chen, “nID-based internet of things and its application in airport aviation risk management,” Chinese Journal of Electronics, vol. 21, no. 2, pp. 209-214, 2012.
12. H. Ning, Y. Fu, S. Hu, and H. Liu, “Tree-Code modeling and addressing for non-ID physical objects in the Internet of Things,” Telecommunication Systems, vol. 58, no. 3, pp. 195-204, 2015.
13. S. Kwok, O. P. Ng, A. H. Tsang, and H. Liem, “Physimetric identification (Physi-ID)–Applying biometric concept in physical object identification,” Computers in Industry, vol. 62, no. 1, pp. 32-41, 2011.

14. M. Beham and S. Roomi, "A review of face recognition methods," International Journal of Pattern Recognition and Artificial Intelligence, vol. 27, no. 04, pp. 1356005101-1356005135, 2013.
15. S. Shaikh and J. Rabaiotti, "Characteristic trade-offs in designing largescale biometric-based identity management systems," Journal of Network and Computer Applications, vol. 33, no. 3, pp. 342-351, 2010. and Technical Research, vol. 3, no. 2, pp. 298-300, 2015.

Disease Symptoms Analysis and Diagnosis System for Physically Challenged Person

Mr. X.Martin Lourduraj
Assistant Professor,
Department of Computer Science and Engineering,
St.Anne's College of Engineering and Technology

Ms.V.Sumitha,
UG Student,
Department of Computer Science and Engineering
St.Anne's College of Engineering and Technology

Ms. D.Jothisri, Ms.E.Kousalya,
UG Students
Department of Information Technology,
Mailam Engineering College, Mailam

Abstract--Context-aware monitoring is an emerging technology that provides real-time personalised health-care services and a rich area of big data application. In this paper, we propose a knowledge discovery-based approach that allows the context-aware system to adapt its behavior in runtime by analyzing large amounts of data generated in ambient assisted living (AAL) systems and stored in cloud repositories. The proposed CAM model facilitates analysis of big data inside a cloud environment. It first mines the trends and patterns in the data of an individual patient with associated probabilities and utilizes that knowledge to learn proper abnormal conditions. The outcomes of this learning method are then applied in context-aware Decision-making processes for the patient. A use case is implemented to illustrate the applicability of the framework that discovers the knowledge of classification to identify the true abnormal conditions of patients having variations in blood pressure (BP) and heart rate (HR).

I. INTRODUCTION

An ambient assisted living (AAL) system consists of heterogeneous sensors and devices which generate huge amounts of patient-specific unstructured raw data every day. Due to diversity of sensors and devices, the captured data also have wide variations. A data element can be from a few bytes of numerical value (e.g. HR = 72 bpm) to several gigabytes of video stream. For example, if we assume a single AAL system generates 100 kilobytes data every second on average then it will become 2.93 bytes in one year. If any system targets to support say, 5 million patients, then the data amount will be 14 bytes per year. Even if a healthcare system targets to analyze only continuous ECG of cardiac patients in real-time inside the cloud environment, then it will produce around 7 Petabytesdata every day from 3.5 million patients. Including these dynamically generated continuous monitoring data there are also huge amounts of persistent data such as patient profile, medical records, disease histories and social contacts.

II. EXISTING SYSTEM

Home health care software sometimes referred to as home care software. Home care software is the application that deals with the storage, retrieval,sharingthe health care information. InExisting System an attribute value set Ai is converted to a numerical value. Some context attributes already have numeric values (e.g. HR, BP, room Temperature). Numerical annotations are used for contexts having nominal value (e.g. activity). The static or historical contexts that have Boolean values (e.g. symptoms) are combined in a single binary string which results a decimal value (e.g. 001100 converted to12).

III. PROPOSED SYSTEM

The proposed System is named as Context-aware monitoring shortly called as CAM.The proposed CAM model facilitates analysis of data inside a cloud environment. It first mines then patterns in the data of an individual patient and utilizes that knowledge to learn proper abnormal conditions. This includes the functionalities of learning and the knowledge discovery process to find patient-specific anomalies using large amounts of data.

3.1 Advantages of Proposed System

✓ Faster learning with greater knowledge.
✓ Reduce the transmission of repeated false alerts.
✓ Innovative architectural model for context-aware monitoring.
✓ Step learning methodology. Demonstrate the performance and efficiency of CAM model.

3.2 Architecture

The general architecture of the proposed knowledge discovery-based context-aware framework for assisted healthcare designed over big data model is visualized . The flow of raw data, context, rules and services between different distributed components are also shown. The overall architecturecan be split into five cloud components. The followingsubsections discuss different components of theframework in brief.

3.2.1 Ambient Assisted Living (AAL) Systems

The big data producers of CAM model are a large number of AAL systems. The low level setup of each system varies according to the requirements of the patient. The sensors, devices and software services of each AAL system produce raw data that contain low level information of a patient's health status, location, activities, surrounding ambient conditions, device status, etc. To learn the daily activity patterns of the patient and the effects of other contexts on his/her medical conditions, all data need to be stored and processed. The high level contexts are obtained from these low level data. The big data scenario of a single AAL system is shown in Figure 3.

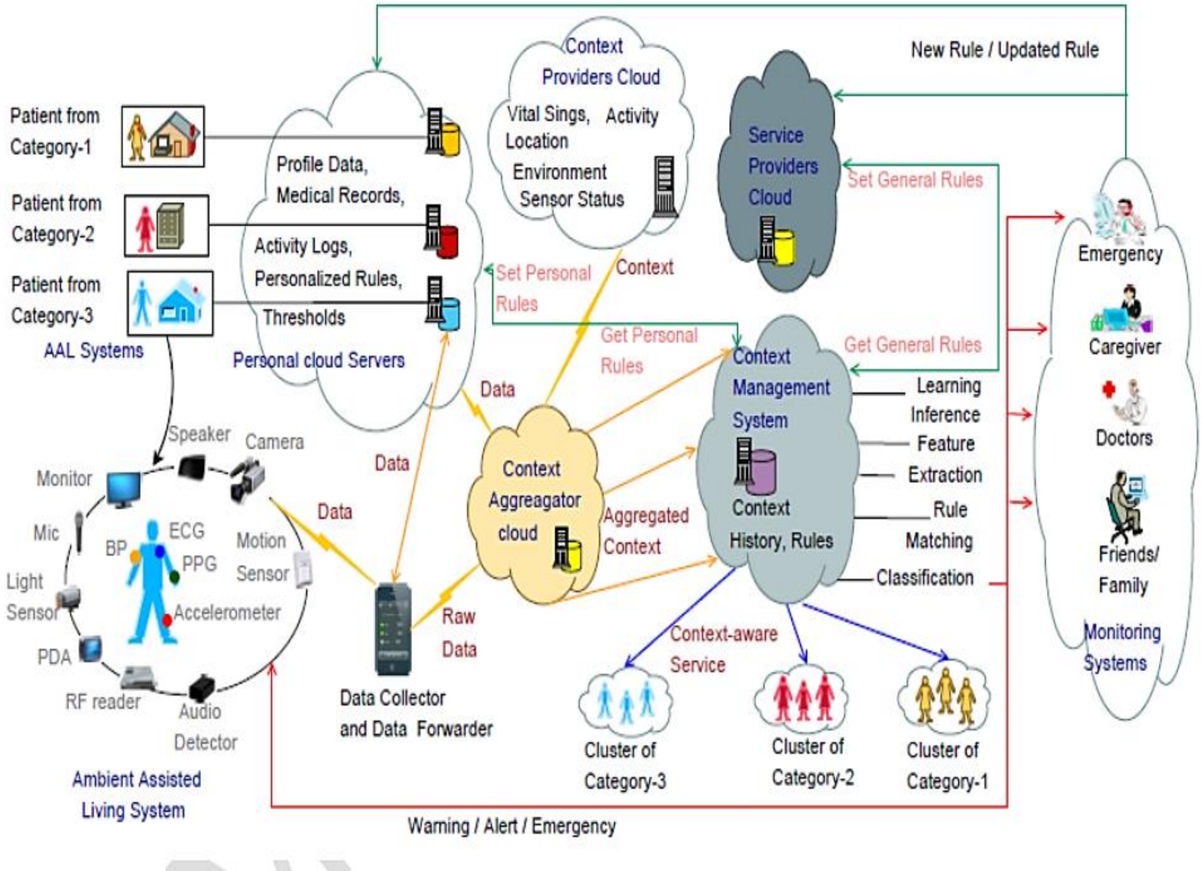


Fig 3.1 Architecture of CAM model

3.2.2 Personal Cloud Servers (PCS)

Each AAL System is connected to a personal cloud server. This is a virtual server in the cloud that is highly scalable and managed by trusted entities. It has secure storage facilities to store patient-specific information such as the profile, recognized patterns of his/her daily activities (e.g. smoking habits), identified threshold values of different vital signs , medication times, disease treatment plans, prescriptions, preferences, emergency contacts and personal medical records. The local processing device in the AAL system can easily exchange information with the PCS. In some cases, the PCS can contain the latest pathological and laboratory test reports, biomedical images or even raw sensor data that is produced in the AAL system. When daily patterns or personalized medical rules are learned, they are stored in the PCS and thus can be retrieved easily when required.

3.2.3 Data Collector and Forwarder (DCF)

Traditional context-aware systems process the low level data and perform the computation in a local server or mobile device and then forward the high level context data to the cloud . But the lack of storage and power in wearable sensors and mobile devices limit them to process large volume of sensor data using decent computational methods. In our proposed model, the job of a local server is only to collect the low level data from the AAL system and forward them directly to the CA or to the PCS. From current knowledge we are assuming that the DCF has the mechanisms to communicate with all sensors and devices that produce raw data. The computations for the conversion from low level data to a high level context are performed inside cloud servers.

3.2.4 Context Aggregator (CA)

The job of the context aggregator (CA) is to integrate all the primitive contexts in a single context state using a context model. Sometimes a single context attribute value as an individual has no meaning if it is not interrelated with other contexts. For example, an increment in HR seems an abnormal condition as a single context, but if the user doing exercise, this can be a normal situation. So, using past and present contexts, it can be determined whether the current user situation is normal or not. Therefore, all the contexts need to be aggregated to classify a situation accurately. The CA does this work and forwards the information to the context management system for the individual user.

3.2.5 Context Providers (CP)

The context providers (CPs) cloud is the main source for generating contexts. The CA distributes the low level data collected from different AAL systems to multiple CPs. Each CP applies well-known techniques to obtain primitive context from the low level data. For example, in applying data mining on accelerometer data it can identify the current activity of the user, using GPS it can identify the location context of the user; it can extract HR value from ECG dataand, so on. CP then delivers the converted contextwith possible high level values to the CA.

3.2.6 Context Management System (CMS)

A Context Management System (CMS) is the core component of the framework. The CMS consists of a number of distributed cloud servers that hold the big data. It stores the context histories of millions of Patients. Different machine learning techniques runinside the CMS that infer different personalizedand generic rules for various user events. When theCMS discovers any personalized rules, they are sent tothe corresponding PCS. Any newly identified genericrules are forwarded to the service provider's (SP)cloud. This is how the CMS keeps every componentof the model up to date with new knowledge. Sometimes,existing rules are required to reason new highlevelknowledge. In that case, CMS uses general rulesfrom SPs or personalized rules from PCSs.After rule generation, the CMS runs another trainingstage, using different data mining algorithms to obtainthe best classifier for a situation classification. Onceoptimized accuracy is achieved, the CMS retains the classifier inside the model to classify any new situation. After classifications, the CMS sends appropriate notification to the monitoring system or to the AALsystem. Using the obtained general behavior, theCMS is also capable of clustering similar groups ofpatients so that they can be covered under the same treatment plan.

3.2.7 Service Providers (SP)

In the CAM model, the service providers are the cloud servers that sustain the generic medical rule to identify various types of diseases and symptoms. The rules of symptoms and anomalous behaviors are continuously updated by medical experts, doctors and other medical service providers. When any new rule is discovered in the CMS it also triggers the change in the SP cloud. The CMS uses rules of SP for data filtering and classification.

3.2.8 Remote Monitoring Systems (RMS)

When the CMS discovers any anomalous pattern in the context for a specific user it sends appropriate notification to the RMS. For example, when the BP level of a patient goes relatively high for a given situation, the CMS alerts the doctor to investigate it, but if it goes abnormally high then the CMS sends alerts to the emergencycenter. Thus, the selection of RMS depends on situation classification. A major goal of our system is to classify a situation correctly to send proper alerts to the right RMS.

3.2.9 Context-Aware Decision Support

The CMS uses the classifier generated in the data mining step to classify forthcoming context states and make context-aware decisions. Based on the classification the CMS performs following actions.

- ✓ If a situation is normal then do nothing.
- ✓ If a situation is abnormal but not dangerous then sends a warning to the user.
- ✓ If any vital context attribute has abnormal value then send alert to doctor.
- ✓ If two or more context attributes are abnormal or anyone is extremely abnormal then notify to emergency.

IV. CONCLUSION

In CAM, a generalized framework for personalized healthcare, which leverages the advantages of context-aware computing, remote-monitoring, cloud computing, machine learning and big data? The system providessolutionas a systematic approach to support the fast-growing communities of people with chronic illness who live alone and require assisted care. The model also simplifies the tasks of healthcare professionals by not swamping them with false alerts. The system canaccurately distinguishemergencies from normal conditions. The data used to validate the model are obtained via artificial data generation based on data derived from real patients, preserving the correlation of a patient's vital signs with different activities and symptoms. The stronger relationship between vital signs and contextual information will make the generated data more consistent and the model will be more accurate for validation. The experimental evaluation of our system in cloud model for patients having different HR and BP levels has demonstrated that the system can predict correct abnormal conditions in a patient with great accuracy and within a short time when it is properly trained with large samples. In future, we intend to extend the model with more context domains.

REFERENCES

1. Pantelopoulos and N. Bourbakis, "A survey on wearablesensor-based systems for health monitoring and prognosis,"IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 40, no. 1, pp. 1–12, 2010.
2. D. N. Monekosso and P. Remagnino, "Behavior analysis for assisted living," IEEE Transactions on Automation Science andEngineering, vol. 7, no. 4, pp. 879–886, 2010.
3. P. Groves, B. Kayyali, D. Knott, and S. Van Kuiken, "The bigdata revolution in healthcare," McKinsey & Company, 2013.

4. S. Pandey, W. Voorsluys, S. Niu, A. Khandoker, and R. Buyya,“An autonomic cloud environment for hosting ecg data analysisservices,” Future Generation Computer Systems, vol. 28, no. 1,pp. 147–154, 2012.
5. A.Ibaida, D.Al-Shammary, and I.Khalil, “Cloud enabled fractalbased ecg compression in wireless body sensor networks”Future Generation Computer Systems, vol. 35, pp. 91–101, 2014.

Trusted Privacy for Mobile User Accessing the Cloud Computing Services

Mr. S.Jerald Nirmal Kumar
Associate Professor,
Department of Computer Science and Engineering,
St. Anne's College of Engineering and Technology

Ms.R.Bowjiya Banu , Ms. P.Pallavi
UG Students,
Department of Computer Science and Engineering
St. Anne's College of Engineering and Technology

Abstract—***In cloud computing, many resources are provided as services on demand over the internet. One of the main services provided by clouds is storage (e.g.,Amazon S3), which allows users to store their large amount of data to the remote clouds without any complex management of storage hardware. But also it inherits many challenges in cloud computing .Privacy has become a considerable issue when the applications of big data are dramatically growing in cloud computing. The benefits of the implementation for these emerging technologies have improved or changed service models and improve application performances in various perspectives. However, the remarkably growing volume of data sizes has also resulted in many challenges in practice. The execution time of the data encryption is one of the serious issues during the data processing and transmissions. In this paper, we concentrate on privacy and propose a novel data encryption approach, which is called Dynamic Data Encryption Strategy (D2ES). Our proposed approach aims to selectively encrypt data and use privacy classification methods under timing constraints. This approach is designed to maximize the privacy protection scope by using a selective encryption strategy within the required execution time requirements.***

Index Terms—Privacy-preserving, data encryption strategy, big data, mobile cloud computing.

I. INTRODUCTION

Due to the deployment of wireless communication technologies and the popularity of mobile devices (such as laptop, intelligent mobile phone, and tablet PC), we can access the Internet services during mobility. This brings much convenience to our daily life as we can enjoy many kinds of network services anywhere and anytime. Despite many benefits of using mobile cloud computing, there are great concerns in protecting data owners' privacy during the communications on social networks or mobile apps [11], [12]. One of the privacy concerns is caused by unencrypted data transmissions due to the large volume of data many applications abandon using cipher texts in mobile cloud data transmissions. This phenomenon can result in privacy leakage issues since plain texts are unchallenging for adversaries to capture information in a variety of ways, such as jamming, monitoring, and spoofing [15]. This privacy issue is exigent because it faces to a contradiction between the security levels and performance that is usually attached to timing constraints.

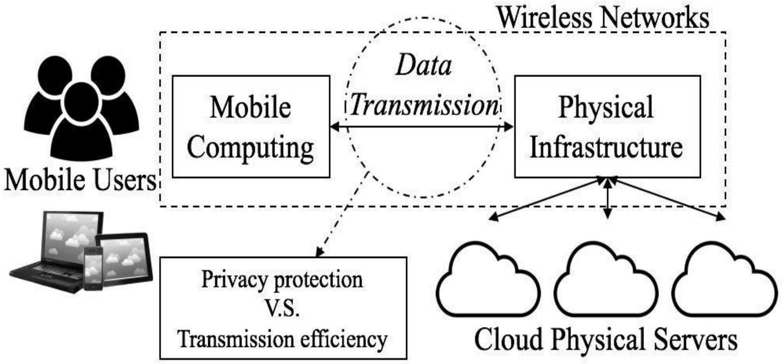


Figure 1.1-MCC Architecture - Balance between privacy protection and transmission efficiency.

This paper addresses the issue of contradictions between data transmission efficiency and protection. To solve the problem, we propose a novel approach that selectively encrypts data in order to maximize the volume of encrypted data under the required timing constraints. The proposed model is called Dynamic Data Encryption Strategy (D2ES) model, which is designed to protect data owners' privacy at the highest level .

II. CONCEPTS AND THE PROPOSED APPROACH

2.1 Problem Definition :

We describe the main research problem in this section. Definition 3.1 shows the identified research problem that is Maximum Data Package under Timing Constraints (MDPuTC) problem.

Maximum Data Package Under Timing Constraints (MDPuTC) Problem: Inputs: data package types fD_ig, the number of data for each data package type N_{Di} , execution time when encrypting data for each single data $T_D{}^{e}{}_{i}$, execution time without encryptions for each single data $T_D{}^{n}{}_{i}$, the privacy weight value for each data type W_{Di} . Outputs: a strategy determining which data will be encrypted. The proposed problem is finding out the approach that can gain the maximum total privacy weight value under a given timing constraint classified into different types, represented as a set fD_ig. The number of data packages in each type D_i is represented as

N_{Di} . Moreover, there are two kinds of execution modes, which include Operation with Encryptions (OwE) and Operation with Non-Encryption (OwNE). The execution time of each data package D_i in OwE mode is $T_D{}^{e}{}_{i}$. Similarly, the execution time of each data package D_i in

OwNE mode is $T_D{}^n{}_i$. Furthermore, we introduce a parameter, Privacy Weight Value (PWV), for each data package type in order to calculate the beneficial acquisitions from encrypting data, represented as W_{Di} .

The meaning of PWV is a criterion showing security signif-icance levels. The acquisitions of PWV values that categorize security issues into multiple levels can be gained by various approaches, such as scorecard sheet [31], [32] and security measurement category [33]. In our proposed model, the PWV value represents the privacy importance for each data package.

Therefore, the output is a encryption strategy that deter-mines which data packages should be encrypted. Assume that the number of encrypted data packages for D_i is $N_D{}^e{}_i$. The object of our research problem is maximizing the sum of PWV values and the objective function is expressed in Eq. (1). In the function, we create a binary function s(i) to represent the selection. The encryption strategy is selected when s(i) = 1 and a non-encryption strategy is selected when s(i) = 0. Since unencrypted data packages do not earn any privacy weights, only encrypted data packages are counted in our model.

$$\text{Output} = \quad \text{Max}(\sum_{s(i)=1} = (N^{e}_{Di} * W_{Di})) = p$$

The condition is the total execution time is no longer than the required timing constraint T_c. The length of T_c must satisfy the following requirement, as shown in Eq. (2). The expression shows the minimum execution time of data operations, which excludes all encryptions.

$$\mathrm{T}c \geq \sum_{s(i)=0} (N_i * T^{n}_{Di})$$

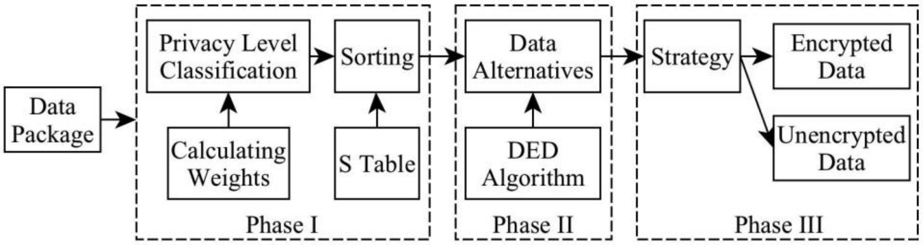
After implementing D2ES approach, some data packages are selected to be encrypted. Configure that the encrypted data set is fD_kg and the non-encrypted data set is fD_jg The total execution time can be gained by Eq. (3):

$$\mathrm{T}_{total} = \sum_{s(i)=1} (N e^{i}_{DK} * Te_{DK}) + \sum_{s(i)=0} (N^{n}_{Dj} * T^{n}_{Dj})$$

Identifying the critical problem is the fundamental of implementing D2ES model. The following section will explain the main mechanism of data alternatives in our model.

2.2 Dynamic Data Encryption Strategy (D2ES) Model :

Based on the definitions given in Section 3.1, we present our D2ES model in this section. The crucial goal of D2ES model is solving the problem defined in Definition 3.1. There are mainly three phases forming the solution. Fig. 2 illustrates three crucial phases of D2ES model.



2.2.1 Phase I: Sorting by Weights:

This is a preparation phase of the model. All data package types are sorted at this phase. The sorting operations consider both execution time and privacy protections; thus, two variables are involved, which are PWVs and the corresponding encryption execution time. For each data package D_i, the value used for sorting operations is defined as a Sorting Weight.

The expression in shows the efficiency of protecting privacy. The sorting operation uses a descending order. The next step is to map all sorting results into a table that is called S Table. The values of the sorting results can determine the priority.

Moreover, in order to improve the level of privacy protec-tion, we introduce a Pairs Matching Collision (PMC) mechanism. This mechanism is designed to avoid the scenario when two plain texts can release users' privacy even though leaking each plain text will not be harmful. The operating principle of PMC mechanism is make sure two pre-defined pair data have at least one data encrypted. The paired data must contain privacy information when they are transmitted or operated in plain texts. Definition 3.2 provides the definition of paired data.

Two data package type Di and Dj. 8Di, if 9 operating Di in plain texts needs a must-encryption operation for Dj, the relation between Di and Dj is a Paired Data, represented as Di $ Dj.

Based on the definition of paired data, we propose a PMC mechanism to ensure that at least one data within the paired data have the encryption priority. Pairs Matching Collision: Any two data Di and Dj matching the requirement of paired data Di $ Dj, the mechanism that can ensure at least one data, Di or Dj, are encrypted is defined as PMC mechanism. The deterministic process of finding out the paired data is a collision.

2.2.2. Phase II: Data Alternatives :

This phase is the crucial step of selecting data packages for encryption operations. We propose the DED algorithm to ac-complish this phase. S Table will be used for providing the reference of protection efficiencies. The operating principle is that data package with higher value of SDi has a higher-level alternative priority than those data packages having lower values of SDi . There are a few sub-steps for selecting data packages.

First, a timing scope needs to be identified. The given timing constraint is Tc. Therefore, the timing scope is [0, Ts], in which the value of Ts can be gained from Eq. (5).

Next, data alternatives are executed. Each encrypted data package's execution time is TDei . We first encrypt the data package with the highest SDi value. The operation will not be ended until two situations occur. The first situation is that all data packages are encrypted. The other situation is that the execution time TDei is longer than the rest of the time.

Define the rest of the execution time is Tr, where Tr 6 Ts. In our model, we calculate time Tr considering both execution time with executions and execution time without encryptions. Once the data package is selected to be encrypted, the execution time without encryption should be added to Tr. Assume that the selected data packages are fDsg. Eq. (6) represents the formulas of calculating Tr.

2.2.3. Phase III: Output :

This phase mainly output an encryption plan deriving from the outcomes of Phase II. Those data with higher-level encryption priority will be selected for the encryptions under a certain constraints. The rest of data will not be encrypted such that plain texts operations are applied.

III. ALGORITHMS

We present the main algorithm used in our D2ES model in this section, which include Dynamic Encryption Determination (DED) algorithm, S Table Generation (STG) algorithm, and Weight Modelization (WM) algorithm. DED algorithm is designed to dynamically select data packages that can be encrypted under certain conditions when considering both timing constraints and facilities' capacities. STG and WM algorithms are designed for supporting DED algorithm.

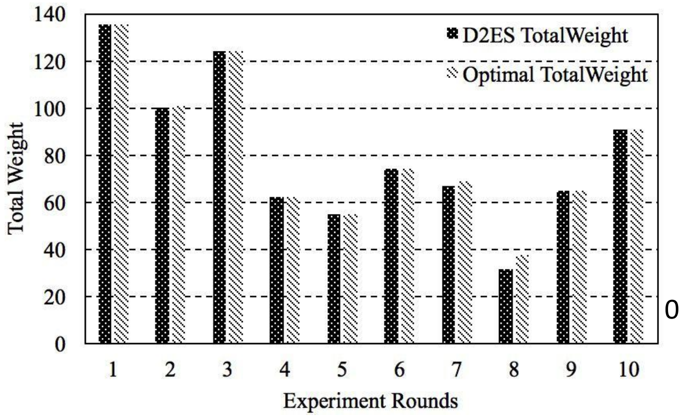
3.1 Dynamic Encryption Determination (DED) Algorithm :

DED algorithm is designed to create the final privacy protection strategy corresponding with the timing constraints and security requirements. Inputs of DED algorithm include M Table, S Table, and T_c. Samples of M Table and S Table are given in Table 1 and 2. The output is the data encryption strategy plan P that directs which data packages need to be encrypted. The crucial part of this algorithm is calculating the remainder of the available time so that the encryption strategy can be determined. Algorithm 5.1 represents the pseudo codes of DED algorithm. The main steps of DED algorithm are illustrated as follows:

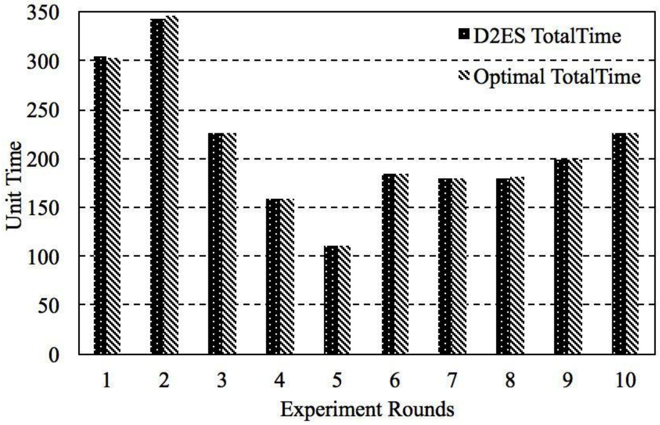
1) Input timing constraint T_c and two tables S Table and M Table. Initialize a strategy plan dataset P as an empty set. Initialize a variable endFlag and assign a False value to it.
2) We use a While loop to create the strategy, which relies on the available time. We estimate whether the data packages should be encrypted one by one in a sequence depend-ing on the priority weights. The data package having a higher-level priority will be determined first.
3) Keep updating the execution time scope T_s. Each data package's non-encryption time needs to be added if the encryption time mode is selected during the process for updating the execution time scope.
4) Add the data package to the set P when the value of T_s is greater than 0 and the encryption time of certain data package is no longer than T_s. This process follows the principle that higher priority weight goes first.
5) End While loop when there is no data package matching the condition any more.

IV. EXPERIMENT AND THE RESULTS

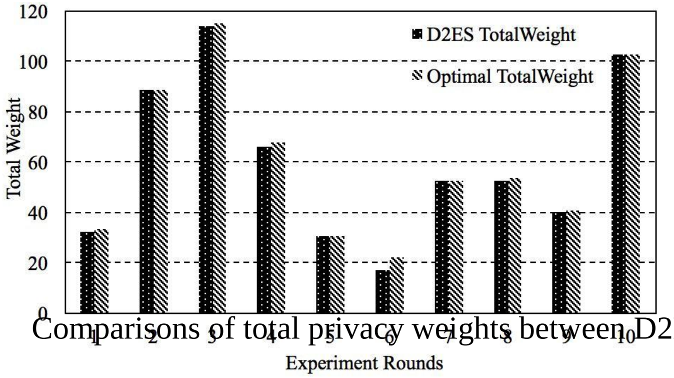
We illustrated our experimental evaluations in this section.



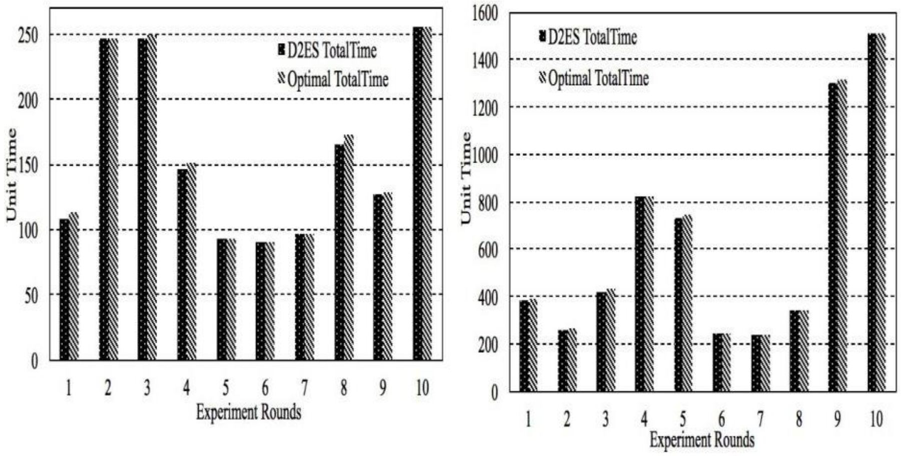
Comparisons of total privacy weights between D2ES and optimal solution under Setting 1.

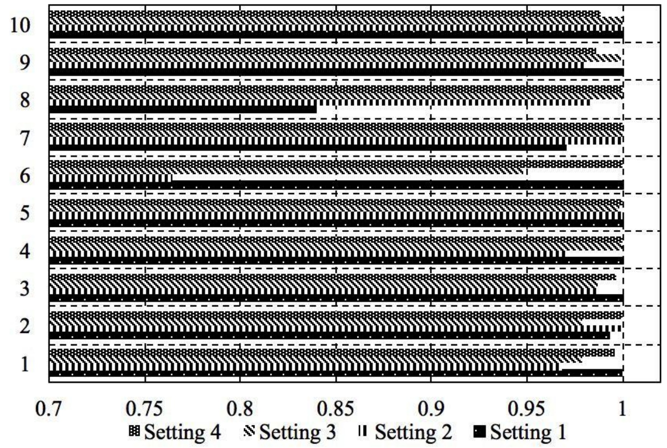


Comparisons of total required execution time between D2ES and optimal solution pairing with Fig. 4 under Setting 1.

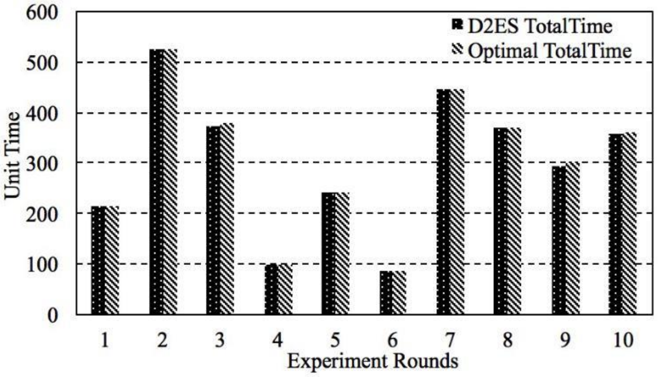


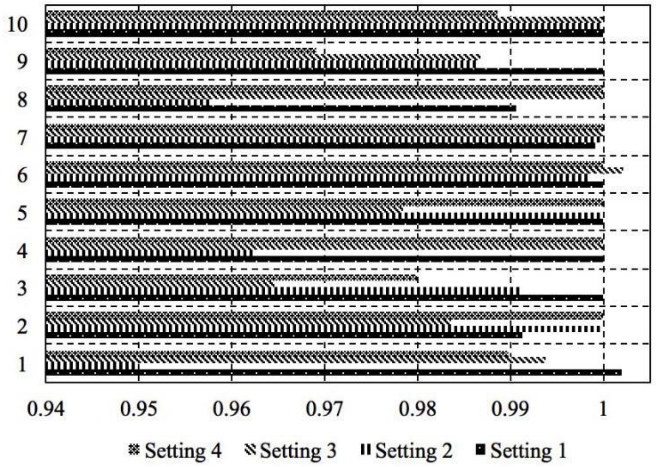
Comparisons of total privacy weights between D2ES and optimal solutions under Setting 2

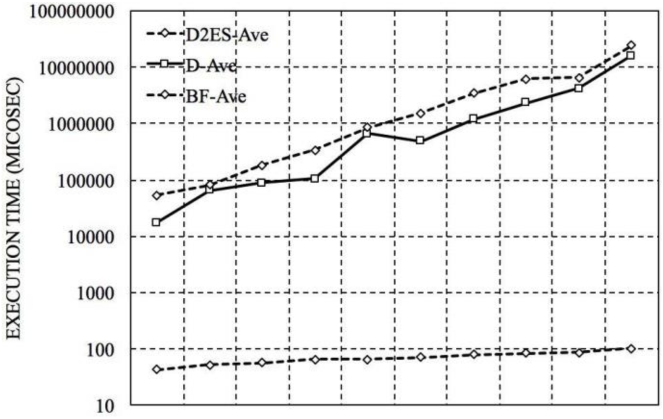




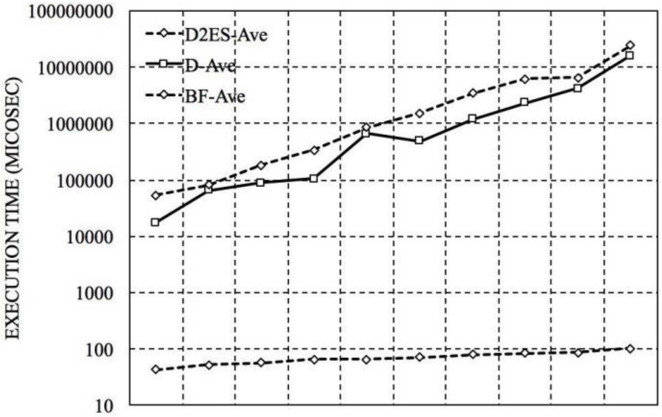
R_p value comparisons of the total privacy weights under Settings 1, 2







Comparisons of average computation time distributions: D2ES, dynamic programming (D), and BF under Setting 1.



V. CONCLUSIONS

This paper focused on the privacy issues of big data and considered the practical implementations in cloud computing. The proposed approach, D2ES, was designed to maximize the efficiency of privacy protections. Main algorithm supporting D2ES model was DED algorithm that was developed to dynamically alternative data packages for encryptions under different timing constraints.

REFERENCES

1. S. Yu, W. Zhou, S. Guo, and M. Guo. A feasible IP traceback framework through dynamic deterministic packet marking. IEEE Transactions on Computers, 65(5):1418–1427, 2016.
2. S. Yu, G. Gu, A. Barnawi, S. Guo, and I. Stojmenovic. Malware propagation in large-scale networks. IEEE Transactions on Knowl-edge and Data Engineering, 27(1):170–179, 2015.
3. S. Liu, Q. Qu, L. Chen, and L. Ni. SMC: A practical schema for privacy-preserved data sharing over distributed data streams. IEEE Transactions on Big Data, 1(2):68–81, 2015.
4. S. Rho, A. Vasilakos, and W. Chen. Cyber physical systems technolo-gies and applications. Future Generation Computer Systems, 56:436– 437, 2016.
5. L. Wu, K. Wu, A. Sim, M. Churchill, J. Choi, A. Stathopoulos, C. Chang, and S. Klasky. Towards real-time detection and tracking of spatio-temporal features: Blob-filaments in fusion plasma. IEEE Transactions on Big Data, 2(3), 2016.
6. S. Maharjan, Q. Zhu, Y. Zhang, S. Gjessing, and T. Basar. Dependable demand response management in the smart grid: A stackelberg game approach. IEEE Transactions on Smart Grid, 4(1):120–132, 2013.
7. M. Qiu, M. Zhong, J. Li, K. Gai, and Z. Zong. Phase-change memory optimization for green cloud with genetic algorithm. IEEE Transactions on Computers, 64(12):3528–3540, 2015.
8. H. Liu, H. Ning, Y. Zhang, Q. Xiong, and L. Yang. Role-dependent privacy preservation for secure V2G networks in the smart grid. IEEE Transactions on Information Forensics and Security, 9(2):208–220, 2014.
9. F. Tao, Y. Cheng, D. Xu, L. Zhang, and B. Li. CCIoT-CMfg: cloud computing and internet of things-based cloud manufacturing service system. IEEE Transactions on Industrial Informatics, 10(2):1435– 1442, 2014.

10. G. Wu, H. Zhang, M. Qiu, Z. Ming, J. Li, and X. Qin. A decentralized approach for mining event correlations in distributed system monitor-ing. Journal of parallel and Distributed Computing, 73(3):330–340, 2013.
11. S. Yu, W. Zhou, R. Doss, and W. Jia. Traceback of DDoS attacks using entropy variations. IEEE Transactions on Parallel and Distributed Systems, 22(3):412–425, 2011.
12. Y. Li, W. Dai, Z. Ming, and M. Qiu. Privacy protection for preventing data over-collection in smart city. IEEE Transactions on Computers, 65:1339–1350, 2015.
13. S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang. Discriminating DDoS attacks from flash crowds using flow correlation coefficient.
IEEE Transactions on Parallel and Distributed Systems, 23(6):1073– 1080, 2012.

Representation of Graphical Description from Natural Language

Mrs.K.Poornambigai,
Assistant Professor,
Department of Computer Science and Engineering,
St. Anne's College of Engineering and Technology, Panruti.

Ms.R.Asha, Ms.A.Gunasudhari, Ms.K.Sonabhrathi, Ms.A.Vimala
UG Students,
Department of Computer Science and Engineering,
St. Anne's College of Engineering and Technology, Panruti.

Abstract- This paper focuses on the mapping of natural language sentences in written stories to a structured knowledge representation. This process yields an exponential explosion of instance combinations since each sentence may contain a set of ambiguous terms, each one giving place to a set of instance candidates. To improve the generalization capacity while learning from a limited amount of annotated data, a new constrained learning algorithm for Bayesian networks is introduced. The effectiveness of the proposed algorithm is evaluated on a set of three stories, yielding nine experiments. Our mapping framework yields performance gains in predicting the most likely structured representations of sentences when compared with a baseline algorithm.

Keywords - Intelligent narrative, natural language processing, structured prediction, constrained learning.

I. INTRODUCTION

The narrative provides a model for communicating experience and culture. Automatically extracting structure information from narrative text is a challenging task. Since the structured representation of connected events and behaviors may involve commonsense inferences based on background knowledge, such as the semantic representation of objects, their properties and behavior, the motivations and goals behind the actions of characters, their emotional outcomes, and the actions they can undertake in the environment.

The SRL aims at a general-purpose semantic representation, i.e. it aims at providing a semantic representation at a higher-level of abstraction, while our work aims at instantiating semantic frame elements at a lower-level of abstraction, in an annotation style tailored for the narrative text.

II. LITERATURE REVIEW

Karl Pichotta and Raymond J. Mooney: Learning Statistical Scripts with LSTM Recurrent Neural Networks. describe a Recurrent Neural Network model for statistical script learning using Long Short-Term Memory, an architecture which has been demonstrated to work well on a range of Artificial Intelligence tasks.

JosepValls-Vargas: Automated Narrative Information Extraction Using Non-Linear Pipelines. propose the use of domain knowledge to improve core NLP task sand the overall performance of our system.

Mark Alan Finlayson: I apply Barwise and Seligman's theory of information flow to understand how sets of signals can carry information. More precisely I focus on the case where the information of interest is not present in any individual signal, but rather is carried by correlations between signals. This focus has the virtue of highlighting an oft-neglected process, viz., the different methods that apply categories to raw signals.

Martha Palmer and Daniel Gildea : The Proposition Bank project takes a practical approach to semantic representation, adding a layer of predicate-argument information, or semantic role labels, to the syntactic.

III. SYSTEM ARCHITECTURE

We have looked into applying existing Natural Language Processing (NLP) techniques to the specific domain of storytelling in order to extract key narrative elements and be able to reuse them for PCG. By addressing these issues expect to be able to develop new frameworks for NLP and PCG that can be used by interactive narrative authors and computer game designers to provide a better experience for their audience.

IV. PROPOSED SYSTEM

The proposed framework starts by extracting a set of cues from the text by using state-of-the-art algorithms for natural language processing (NLP) see the blocks Syntactic Processing, SRL and Co-reference Resolution. This information is encoded in an XML file that is provided to the Mapping to KR module, which also receives the allowable variable values, i.e. the domain.

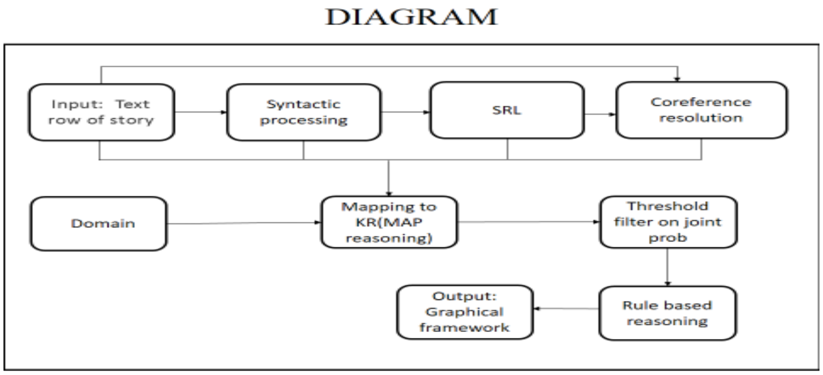


Figure 4.1- Proposed system

V. CONCLUSION

In this work, we introduced a framework to map text from written stories to a specific low-level KR. This new frame-work is able to reason with uncertainty, to integrate training from annotated data and constraints encoding information on mutually exclusive values, beyond evidence from external sources, such as information from the language model . Similar to other methods for structured prediction, the mapping aims at predicting the most likely structure by searching in the large search space derived from the exponential explosion of instance combinations, i.e. MAP inference.

VI. FUTURE SCOPE

Learning the text and rearrange the text and mail for priority based. Most of the company need to work priority based task .Priority scheduling is a method of scheduling processes based on priority. In this method, the scheduler chooses the tasks to work as per the priority, which is different from other types of scheduling, for example, a simple round robin.

REFERENCES

1. Martha Palmer, Daniel Gildea, and Nianwen Xue. Semantic role labeling. Synthesis Lectures on Human Language Technologies, 3(1):1–103, 2010.
2. Charu C Aggarwal and Cheng Xiang Zhai. Mining Text Data. Springer Science & Business Media, 2012.
3. Martha Palmer, Daniel Gildea, and Paul Kingsbury. The proposition bank: An annotated corpus of semantic roles. Computational Linguistics, 31(1):71–106, 2005.
4. Collin F Baker, Charles J Fillmore, and John B Lowe. The berkeley framenet project. In Proceedings of the 17th International Conference on Computational Linguistics-Volume 1, pages 86–90, 1998.
5. Xavier Carreras and Llu´ıs Marquez`. Introduction to the conll-2005 shared task: Semantic role labeling. In Proceedings of the Ninth Conference on Computational Natural Language Learning, pages 152–164, 2005.
6. Vincenzo Lombardo and Antonio Pizzo. Ontology based visualization of characters intentions. In Alex Mitchell, Clara Fernndez-Vara, and David Thue, editors, Interactive Storytelling, volume 8832 of Lecture Notes in Computer Science, pages 176–187. 2014.
7. Ruqian Lu and Songmao Zhang. Automatic generation of computer animation: using AI for movie animation. Springer-Verlag, 2002.

Aadhar Card Verification Based Online Polling

Mrs. S Sahunthala
Assistant Professor,
Department of Information Technology,
Anand Institute of Higher Technology.

Mr.K Charan, Mr.S Manikandan, Mr.D Ruthramoorthy
UG Students
Department of Information Technology,
Anand Institute of Higher Technology.

Abstract- Online polling system is the system which enables user to vote online. Specifically, the Voting system consisted of server services which are each linked with a database for storing persistent data. . Voters can also use the services to log into the electronic voting system website. The field officer will send the voter information and their voting's and that information will be maintained by author card verification. Admin will maintain all information regarding voter and counts automatically their voting's for their selected parties' .An online voting system for Indian election is proposed for the first time in this paper. The proposed model has a greater security in the sense that voter high security with One Time Password is implemented before the vote is accepted in election commission of India main database .The additional feature of the model is that the voter can confirm if his/her vote has gone to correct candidate/party.

Index Terms - Security, OTP, verification

I. INTRODUCTION:

Electronic voting (also known as e-voting refers to voting using electronic means to either aid or take care of the chores of casting and counting votes. Depending on the particular implementation, e-voting may use standalone electronic voting machines (also called EVM) or computers connected to the Internet. It may encompass a range of Internet services, from basic transmission of tabulated results to full-function online voting through common connectable household devices. The degree of automation may be limited to marking a paper ballot, or may be a comprehensive system of vote input, vote recording, data encryption and transmission to servers, and consolidation and tabulation of election results. A worthy e-voting system must perform most of these tasks while complying with a set of standards established by regulatory bodies, and must also be capable to deal successfully with strong requirements associated with security, accuracy, integrity, swiftness, privacy, auditability, accessibility, costeffectiveness, scalability and ecological sustainability.
Electronic voting technology can include punched cards, optical scan voting systems and specialized voting kiosks (including self-contained direct-recording electronic voting systems, or DRE). It can also involve transmission of ballots and votes via telephones, private computer networks, or the Internet.

In this paper a person can also vote from outside of his/her allotted consistiuency or from his/her preferred location. In the proposed system the tallying of votes will be done automatically thus saving a huge time and enabling election commissioner of India to announce the result within a very short period. Voting schemes have evolved from counting voting technique, and also it provides improved features of voting system over traditional voting system such as accuracy, convenience, flexibility, privacy, verifiability and mobility. But it suffers from various drawbacks such as Time consuming , Consumes large volume of pare work , No direct role for the higher officials, Damage of machines due to lack of attention, Mass update doesn't allows users to update and edit many item simultaneously. These drawbacks are overcome by Online Voting System. Online Voting System is a voting system by which any Voter can use his/her voting rights from anywhere in the country. We provide a detailed description of the functional and performance characteristics of online voting system. Voter can cast their votes from anywhere in the country without visiting to voting booths, in highly secured way. That makes voting a fearless of violence and that increases the percentage of voting.

The authenticating voters and polling data security aspects for e-voting systems are discussed here. It ensures that vote casting cannot be altered by unauthorized person. The voter authentication in online e-voting process can be done by formal registration through administrators and by entering OTP Certificate. In Offline e-voting process authentication can be done using facial recognization, fingerprint sensing and RFID (smart cards) which enables the electronic ballot reset for allowing voters to cast their votes. Also the voted data and voters details can be sent to the nearby Database Administration unit in a timely manner using GSM System with cryptography technique.

In the present day, democracy has become an important part of people's lives, and to achieve democracy must meet several conditions. The heart of democracy is voting. The heart of voting is trust that each vote is recorded and tallied with accuracy and impartial it. The accuracy and impartiality are tallied in high rate with biometric system. Among these biometric signs, fingerprint has been researched the longest period of time, and shows the most promising future in real-world applications. Because of their uniqueness and consistency over time, fingerprints have been used for identification over time. Voting theory began formally in the 18th century and many proposals for voting systems have been made ever since. There have been several studies on using electronic technologies to improve elections. When designing an electronic voting system, it is essential to consider ways in which the voting tasks can be performed electronically without sacrificing voter privacy or introducing opportunities for fraud. An electronic voting system defines rules for valid voting and gives an efficient method of counting votes, which re aggregated to yield a final result. Moreover, electronic voting systems can improve voter identification process by utilizing biometric recognition.

Though EVM manufacturers and election officials have attempted to keep the design of the EVMs secret, this presents only a minor obstacle for would-be attackers. There are nearly 1.4 million EVMs in use throughout the World and criminals would only need access to one of them to develop working attacks. Dishonest insiders or other criminals would likely face less difficulty than we did in obtaining such access. There are many other possibilities for manipulating Indian EVMs, both with and without the involvement of dishonest election insiders. Depending on the local context and security environment, the nature and scale of potential manipulations may vary, but neither the machines' simplicity nor their secret design keeps themSafe. This study establishes that the EVMs used in India are not tamper-proof and are susceptible to a range of attacks. The use of similar paperless DREs has been discontinued in California [9], Ireland [1] Indian election authorities should immediately review the security procedures now in place and should inspect all EVMs for evidence of fraud. Moving forward, India should consider adopting a voting system that provides greater security and transparency, such as paper ballots.

Elections enable every citizen of the country to participate in the process of government formation. The constitution of India provides for an election commission of India which is responsible for superintendence direction and control of all elections. Integrity of election process will determine the integrity of democracy itself. So the election system must be secure against a variety of fraudulent behaviors and should be transparent and comprehensible that voters can accept the result of an election. [4] in this paper section 2 we describe the literature review

II. LITERATURE REVIEW

A wide variety of systems requires reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user and no one else. Examples of such applications include secure access to buildings, computer systems, laptops, cellular phones, and ATMs. In the absence of robust personal recognition schemes, these systems are vulnerable to the wiles of an impostor. Biometric recognition, or, simply, biometrics, refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics. By using biometrics, it is possible to confirm or establish an individual's identity based on "who she is", rather than by "what she possesses" (e.g., an ID card) or "what she remembers" (e.g., a password). We give a brief overview of the field of biometrics and summarize some of its advantages, disadvantages, strengths, limitations, and related privacy concerns.

With the evolution of consumer electronics technologies, personal information in consumer devices is becoming increasingly valuable. To protect private information from misuses due to loss or theft, secure user identification mechanisms should be equipped into the consumer devices. This paper develops a secure user identification system for consumer electronics devices based on fingerprint identification. The fingerprint identification system is one of the biometric sensor technologies, which provides high accuracy and convenience than other identification techniques. Specifically, the proposed system uses the orientation map and the edit-distance for immediate and accurate identification of users. Experimental results show that the proposed system achieves good performance in terms of the false rejection rate and the false acceptance rate.

The problem of voting is still critical in terms of safety and security. This paper deals with the design and development of a web-based voting system using fingerprint in order to provide a high performance with high security to the voting system also we use web technology to make the voting system more practical. The new design is proposed an election for a university for selecting the president of the university. The proposed EVS allows the voters to scan their fingerprint, which is then matched with an already saved image within a database. The software is implemented completely as a .net managed code in C#. Upon completion of voter identification, voters are allowed to cast their vote using voting website. Casted vote will be updated immediately. The result shows that the proposed electronic voting system is fast, efficient and fraud-free.

In this paper, we present a security analysis of a real Indian EVM obtained from an anonymous source. We describe the machine's design and operation in detail, and we evaluate its security, in light of relevant election procedures. We conclude that in spite of the machine's simplicity and minimal software trusted computing base, it is vulnerable to serious attacks that can alter election results and violate the secrecy of the ballot. We demonstrate two attacks, implemented using custom hardware, which could be carried out by dishonest election insiders or other criminals with only brief physical access to the machines. This case study contains important lessons for Indian elections and for electronic voting security more generally.

III. PROPOSED MODEL AND METHOD

In this proposed system, the voting system primarily entails the physical and administrative separation of the electoral register and electronic ballot box. Specifically, the. Voting system consisted of server services which are each linked with a database for author card verification and mobile number verification. . Voters can also use the services to log into the electronic voting system website by using these both authentication process. The field officer will send the voter information and their voting's and that information will be maintained by author card and mobile number verification. Admin will maintain all information regarding voter and counts automatically their voting's for their selected parties.

3.1 Proposed Model:

In this model the online voting system had Saved Ballot Templates eliminate the need to configure elections from scratch. Just do it once, then save that ballot configuration, and in subsequent years, specify only the names of the candidates are shown to the voters. But in proposed model the voter can able to see all the details of the candidates. Reduced costs are enjoyed when the expenses of printing, mailing and tabulating paper ballots are lessened or even eliminated entirely from the election process.

The figure 1 proposed system model explains about the AADHAR card verification base online polling .The admin / voter should login with their own AADHAR card for their verification of election commission of India. If the voters sign in to the voting machine with the AADHAR card .The candidate information will be stored in server of election commission of India for authentication .Then the verification process will carried out for the voters by generating a One Time Password to their valid mobile number .If the voters enter the OTP (4 digit number) in the voting machine .Then the voter can be able to vote for their candidates. If the OTP entered was incorrect then the voter cannot able to vote.

3.2 Steps to Implement The Proposed Model

```
Step1:- set of input users. (17….n)
Step2:-store the user information in the database.
    For I range 1 to n
Step3:-verifying aadhar card number, finger print, if it is true then generate OTP else return false.
Step4:- if OTP is true eligible vote, else return false.
    End for
```

3.3 Phases of the System

We propose client-server web-enabled software architecture for the project. On the client side we have a fingerprint scanner and a GUI that accepts voter's AADHAR number, and mobile number that provides an interface to vote and display confirmation through One Time Password, status and error messages are also displayed through messages. The GUIs will only act on events from the server and feedback of the voter without any extra processing. Servers are placed at remote locations from the poll booths. They are used for carrying out all the processing work such as image processing, transferring data between the client and the database, generating statistics, sending messages to voters, etc. All the zonal databases retrieve data from CIDR of only those people who come under its scope. This data is periodically updated and is stored in volatile form so that it can be erased if and when necessary such as during security attacks, natural calamities, maintenance works, etc.

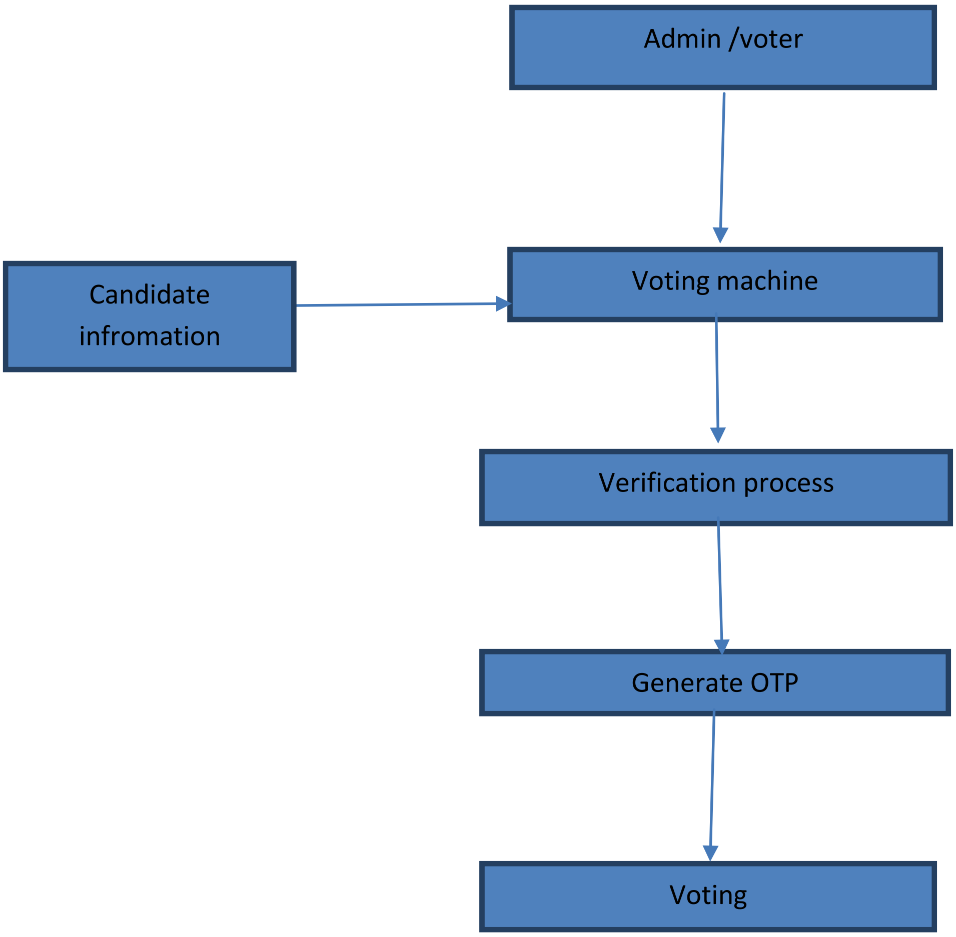


Figure 3.1- Proposed system model

3.3.1 Authentication And Verification Of The Vote

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In order to authenticate a person we require them to have a valid UID number. The number will be checked in the local database records first. If it is not found then it will search the central repository again it's not found then the mobile number authentication process will carried out. It involves one-to-many match. If the person's number is not found in the central database or with a valid mobile number then of course s/he will be devoid of taking part in the voting process. On the other hand if the number is present in the central database then the data of that person will be cached to the zonal database. This record is extracted from the local database and sent to authenticating servers for further processing. For verification the person's fingerprint will be scanned at the client-side and matched one-to-one at the servers with the data extracted from the local database and another verification of mobile number through OTP(One Time Password) will be send and the candidate enters the password matching process will be done. This process puts less stress on the local database and improves data traffic.

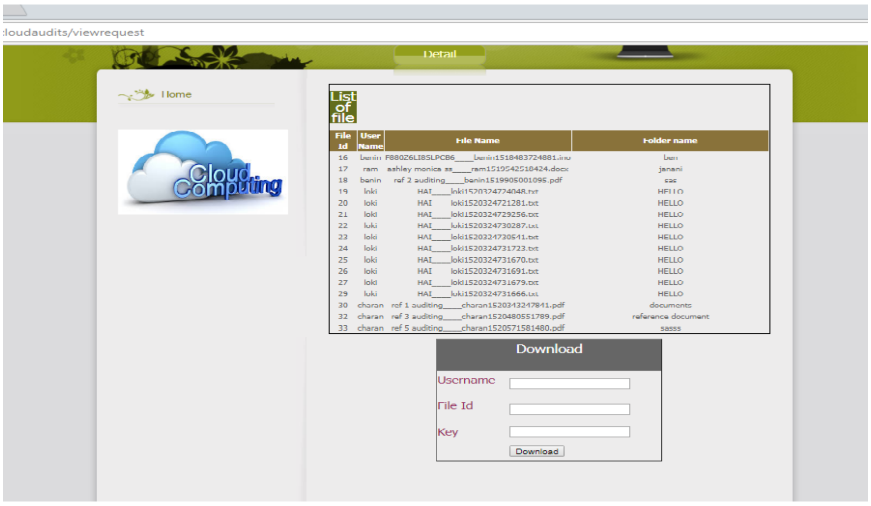
3.3.2 Preventing Fraudulent Voting

The first and the leading thing to guarantee proper voting is by accurately validating every voter. It is essential to identify that every person coming to vote is unique otherwise it will violate the very principle of voting. Any person would be voting on behalf of others. Fingerprint matching ensures the authentication that the system requires. However in order to improve accuracy it is important to keep false reject rate (FRR) and false accept rate (FAR) as low as possible; practically close to zero. To prevent underage individuals from voting, the system calculates person's age from the birth date present in the database records. If the calculated age is above permissible limit the person is allowed to vote and prevented otherwise. To prevent voters from voting two or multiple times we implement voting flags in the local databases. This flag is initially set to false.

3.3.3 Generating Report

Whenever a voter casts a vote in favour of the candidate of choice, the vote count of that candidate gets incremented in the local database. The votes from all the local databases are summed up to get the final figure that the candidate has received .Thus this system provides instantaneous results and prevents unnecessary use of manpower and wastage of time. Since this is an electronic system and uses digital data it has several advantages. Statistics can be generated from the obtained data for e.g. we could answer how many people have voted from a certain region, how many females voted, which age group voted the most, the highest turnouts, comparisons from previous years, etc. all that was not possible from traditional voting methods not even from EVMs. It would provide important insights into the election results and help improve the system even further.

IV. EXPERIMENTAL



List of file

File Id	User Name	File Name	Folder name
16	benin	F880Z6LI8SLPCB6____benin1518483724881.inu	ben
17	ram	ashley monica ss____ram1519542518424.docx	janani
18	benin	ref 2 auditing____benin1519905001095.pdf	sas
19	loki	HAI____loki1520324724048.txt	HELLO
20	loki	HAI____loki1520324721281.txt	HELLO
21	loki	HAI____loki1520324729256.txt	HELLO
22	loki	HAI____loki1520324730287.txt	HELLO
23	loki	HAI____loki1520324730541.txt	HELLO
24	loki	HAI____loki1520324731723.txt	HELLO
25	loki	HAI____loki1520324731670.txt	HELLO
26	loki	HAI____loki1520324731691.txt	HELLO
27	loki	HAI____loki1520324731679.txt	HELLO
29	loki	HAI____loki1520324731666.txt	HELLO
30	charan	ref 1 auditing____charan1520313247841.pdf	documents
32	charan	ref 3 auditing____charan1520480551789.pdf	referance document
33	charan	ref 5 auditing____charan1520571581480.pdf	sasss

Download

Username
File Id
Key

Figure 4.1 OTP generation to the election person

This election model implemented java with mysql .All user information stored in my sql .sampp tool generate OTP to the election person this OTP rise the security in the election commission. The figure shows OTP generation by sampp to the election person's mobile number only one mobile number is allowed for each person in the election commission. If the person try to vote same mobile number he/she not elgible to vote. Our model works on any platform .

V. CONCLUSION

This paper describes the proposed model for online voting system for India .the proposed system is much secure and efficient than traditional voting system. Manipulation of votes and delay of results can be avoided easily .now a days the duplicate votes are increased to 40% in India and 10% who are not voting. Totally only 50% votes are received to the election commission of India. To increase the voting rate in a secure manner , which a unique ADHAAR identity and mobile number identification is the centre point of our proposed model .It leads to the easier verification of both voters and candidate. In the proposed framework, we have tried to build a secure online voting system that is free from unauthorised access while casting votes by the voters .The server aspects of the proposed system have such distribution of authority that server does not enable to manipulate the votes .It is expected that the proposed online voting system will increase the transparency and reliability of the existing electoral system.

REFERENCES

1. Ankit Anand1, Pallavi Divya2, an E_cient Online Voting System, Vol.2, Issue.4, July-Aug. 2012, pp-2631-2634.
2. Alaguvel.R1,Gnanavel.G2,Jagadhambal.K3, Biometrics Using Electronic Voting System With Embedded Security, Vol. 2,Issue 3,March 2013.
3. Firas I. Hazzaa1, Seifedine Kadry2, OussamaKassem Zein3, Web-BasedVoting System Using Fingerprint: Design and Implementation, Vol. 2, Issue.4, Dec 2012.
4. Malwade Nikita1, Patil Chetan2, Chavan Suruchi3, Prof. Raut S. Y4, Secure Online Voting System Khasawneh Proposed By Biometrics And Steganography, Vol. 3, Issue 5, May 2013.
5. M., Malkawi, M., & Al-Jarrah, O. (2008). A Biometric-Secure e-Voting System for Election Process.Proceeding of the 5th International Symposium on Mechatronics and its Applications (ISMA08). Amman, Jordan.
6. Prasad, H. K., Halderman, A. J., &Gonggrijp, R. (Oct. 2010). Security Analysis of India's Electronic Voting Machines. Proc. 17th ACM Conference on Computer and Communications Security (CCS '10).
7. UIDAI. (2012). Role of Biometric Technology in Aadhaar Authentication.
8. Yinyeh, M. O., &Gbolagade, K. A. (2013). Overview of Biometric Electronic Voting System in Ghana.International Journal of Advanced Research in Computer Science and Software Engineering.
9. McGaley, Margaret. "Irish Citizens for Trustworthy Voting." 6 July 2004. http://evoting.cs.may.ie/

Privacy Preserved Framework for Utility Services in Cloud

Mr.S.Jerald Nirmal Kumar,
Associate Professor,
Department of Computer Science and Engineering,
St. Anne's College of Engineering and Technology,

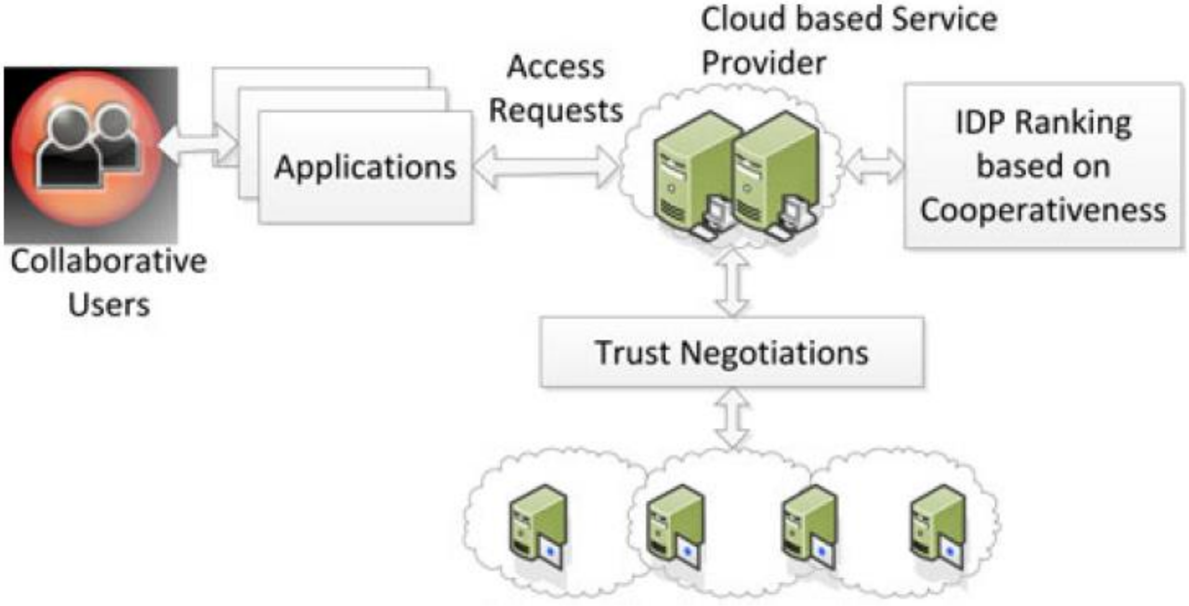
Mr.S.Salman, Mr. R.Rajeswaran, Mr. J.Muthu,
UG Students,
Department of Computer Science and Engineering,
St. Anne's College of Engineering and Technology.

Abstract—Utility based cloud services can efficiently provide various supportive services to different service providers. Trust negotiations with federated identity management are vital for preserving privacy in open systems such as distributed collaborative systems. However, due to the large amounts of server based communications involved in trust negotiations scalability issues prove to be less cumbersome when offloaded on to the cloud as a utility service. In this view, we propose trust based federated identity management as a cloud based utility service. The main component of this model is the trust establishment between the cloud service provider and the identity providers. We propose novel trust metrics based on the potential vulnerability to be attacked, the available security enforcements and a novel cost metric based on policy dependencies to rank the cooperativeness of identity providers. Practical use of these trust metrics is demonstrated by analyses using simulated data sets, attack history data: published by MIT Lincoln laboratory, real-life attacks and vulnerabilities extracted from Common Vulnerabilities and Exposures (CVE) repository and fuzzy rule based evaluations. The results of the evaluations imply the significance of the proposed trust model to support cloud based utility services to ensure reliable trust negotiations using federated identity management.

I. INTRODUCTION

Trust negotiations are necessary to control the users' access to information resources in open systems [1]. In a trust negotiation process, two parties who are unknown to each other, establishes trust through an iterative bilateral exchange of credible digital identities. Collaborations often persist over a limited time period, and therefore, ii)organizational restrictions for inclusion of these collaborative users into their local security policies. Digital identity management (IDM) is vital to facilitate reliable and seamless trust negotiations. Among the various identity management approaches, federated identity management is considered to be more appropriate for distributed collaborative environments. During a trust negotiation process, identity providers (IDPs) verify and provide necessary digital identities upon request. Trust is used to interpret the reliability in order to convince that an entity (e.g. user, server, system component) is secure or accurate [3]. However, specific definition of trust depends on the application. In this paper, we use trust to denote the reliability of the identity providers to the CSP, in terms of the i) cooperation of IDPs in releasing identities without prolonged delays as well as ii) the ability to release identities without failure in view of potential attacks.

II. MODULE DESCRIPTION


Cloud based Service Provider
Access Requests
Applications
IDP Ranking based on Cooperativeness
Collaborative Users
Trust Negotiations

2.1. Digital Identity Management

As more and more activities and processes such as shopping, discussion, entertainment and business collaboration are conducted in the cyber world, digital identities, be them user names, passwords, digital certificates, or biometric features and digital identity management have become fundamental to underpinning accountability in business relationships, controlling the customization of the user experience, protecting privacy, and adhering to regulatory controls. In its broadest sense, identity management revolves around the enterprise process of adding or removing (provisioning) digital identity information and managing their authentication and associated access rights (policy) to information systems and applications ("access management").

2.2. Federation Identity Management

Federated identity management (FIM) is an arrangement that can be made among multiple enterprises to let subscribers use the same identification data to obtain access to the networks of all enterprises in the group. The use of such a system is sometimes called identity federation.federated identity management as a cloud based utility service. The main component of this model is the trust establishment between the cloud service and DSA algorithm for security to client information. we use trust to denote the reliability of the identity providers to the CSP, in terms of the i) cooperation of IDPs in releasing identities without prolonged delays as well as ii) the ability to release identities without failure in view of potential attacks**.** Identity federation links a user's identity across multiple security domains, each supporting its own identity management system. When two domains are federated, the user can authenticate to one domain, and then access resources in the other domain without having to log in a second time.Identity federation offers economic advantages, as well as convenience, to enterprises and their network subscribers. For example, multiple corporations can share a single application, with resultant cost savings and consolidation of resources. Single sign-on (SSO) is an important component of identity federation, but it is not the same as identity federation. In order for FIM to be effective, the partners must have a sense of mutual trust. Authorization messages among partners in an FIM system can be transmitted using Security Assertion Markup Language (SAML) or a similar XML standard that allows a user to log on once for affiliated but separate Web sites or networks.

2.3. Identity Management

Identity management includes authenticating users and determining whether they're allowed access to particular systems. ID management works hand-in-hand with identity access management systems. Identity management is focused on authentication, while access management is aimed at authorization.ID management determines whether a user has access to systems, but also sets the level of access and permissions a user has on a particular system. For instance, a user may be authorized to access a system but be restricted from some of its components. The main goal of identity management is to ensure that only authenticated users are granted access to the specific applications, systems or IT environments for which they are authorized. This includes control over user provisioning and the process of onboarding new users such as employees, partners, clients and other stakeholders. Identity management also includes control over the process of authorizing system or network permissions for existing users and the off boarding of users who are no longer authorized to access organization systems. Identity governance, the policies and processes that guide how roles and user access should be administered across a business environment, is also an important aspect of identity management. Identity governance is key to successfully managing role-based access management systems. Identity management is an important part of the enterprise security plan, as it is linked to both the security and productivity of the organization. In many organizations, users are granted more access privileges than they need to perform their functions. Attackers can take advantage of compromised user credentials to gain access to organizations' network and data. Using identity management, organizations can safeguard their corporate assets against many threats including hacking, ransomware, phishing and other malware attacks. Identity management systems can add an additional layer of protection by ensuring user access policies and rules are applied consistently across an organization. An identity and access management (IAM) system can provide a framework that includes the policies and technology needed to support the management of electronic or digital identities. Many of today's IAM systems use federated identity, which allows a single digital identity to be authenticated and stored across multiple disparate systems.

III. TECHNIQUES

3.1. DSA Algorithm

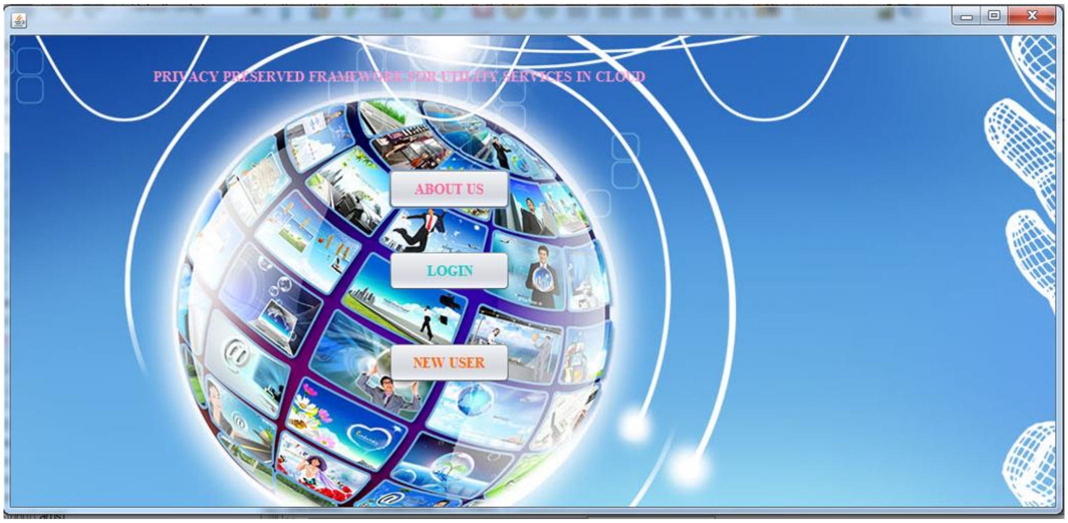
DSA, most digital signature types are generated by signing message digests with the private key of the originator. This creates a digital thumbprint of the data. Since just the message digest is signed, the signature is generally much smaller compared to the data that was signed. As a result, digital signatures impose less load on processors at the time of signing execution, use small volumes of bandwidth, and generate small volumes of ciphertext intended for cryptanalysis.

DSA, on the other hand, does not encrypt message digests using private key or decrypt message digests using public key. Instead, it uses unique mathematical functions to create a digital signature consisting of two 160-bit numbers, which are originated from the message digests and the private key. DSAs make use of the public key for authenticating the signature, but the authentication process is more complicated when compared with RSA.

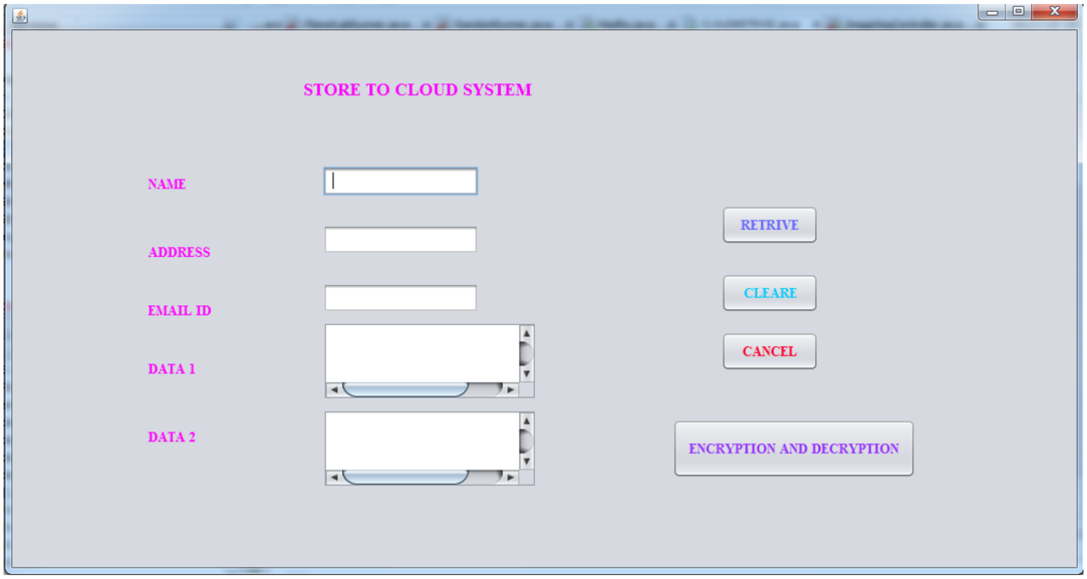
The digital signature procedures for RSA and DSA are usually regarded as being equal in strength. Because DSAs are exclusively used for digital signatures and make no provisions for encrypting data, it is typically not subject to import or export restrictions, which are often enforced on RSA cryptography.

IV. OUTPUT

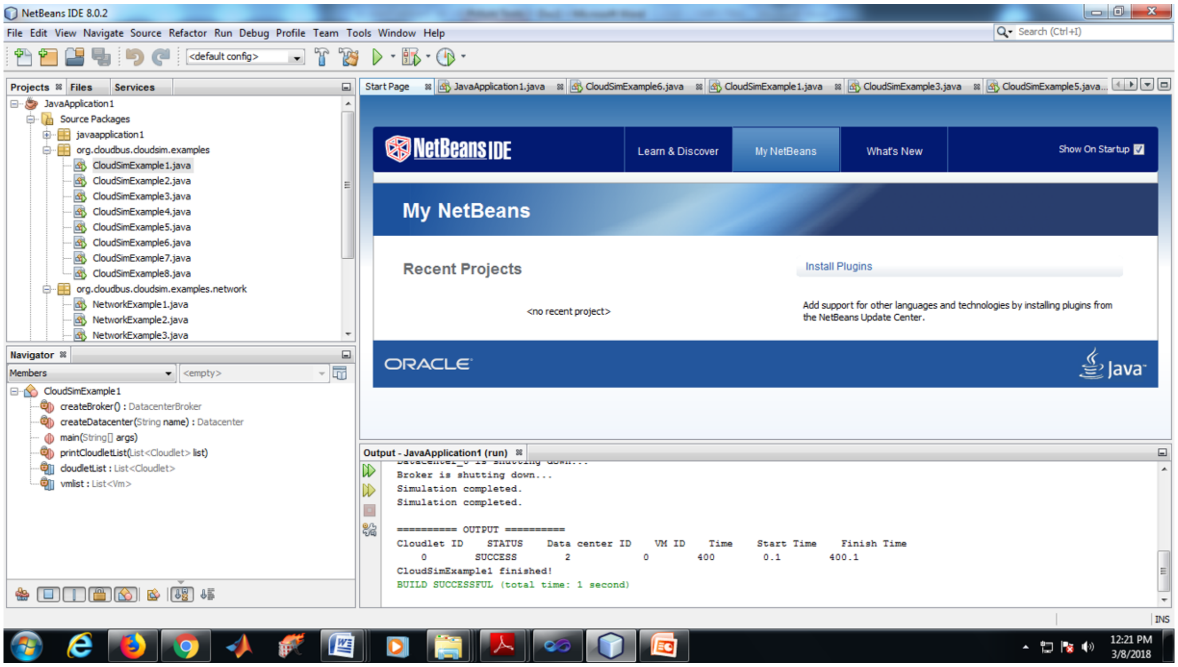
4.1. Sign Up Page



4.2. User Details



4.3. Simulator



```
Datacenter_0 is shutting down...
Broker is shutting down...
Simulation completed.
Simulation completed.

========== OUTPUT ==========
Cloudlet ID    STATUS    Data center ID    VM ID    Time    Start Time    Finish Time
    0         SUCCESS         2              0        400        0.1         400.1
CloudSimExample1 finished!
BUILD SUCCESSFUL (total time: 1 second)
```

V. CONCLUSION

In this paper we have proposed a trust based federated identity management model as a cloud based utility service for distributed collaborative services. In this model the most important aspect is the trust establishment between the identity providers and the requesting server on the application side. We have proposed novel trust metrics based on the threat vulnerability, security enforcements and a policy based cost metric. We have demonstrated how these trust metrics can be computed by using real life attack history data, mitigation and detection techniques, recently discovered vulnerabilities using fuzzy arithmetic and fuzzy rule based inference models. The results prove the viability of the proposed cloud based utility service model as a reliable mechanism to facilitate trust negotiations using federated identity management. It also intrigues more work in a direction with real world implementations for mobile services with service dependent security and privacy requirements.

REFERENCES

1. E. Bertino, E. Ferrari, and A. Squicciarini, "Trust negotiations: Concepts, systems, and languages," Comput. Sci. Eng., vol. 6, no. 4, pp. 27–34, 2004.
2. E. Bertino, L. D. Martino, F. Paci, and A. C. Squicciarini, "Digital identity management and trust negotiation," in Security for Web Services and Service-Oriented Architectures. New York, NY, USA: Springer, 2010, pp. 79–114.
3. A. Nagarajan and V. Varadharajan, "Dynamic trust enhanced security model for trusted platform based services," Future Generation Comput. Syst., vol. 27, no. 5, pp. 564–573, 2011.

Smart ATM Security System Using Wireless Pin Authentication Method

Ms.V. Varalakshmi
Assistant Professor,
Department of Computer Science and Engineering,
St. Anne's College of Engineering and Technology

Ms.J.Monisha, Ms.M.Dhanalakshmi
UG students
Department of Computer Science and Engineering,
St. Anne's College of Engineering and Technology.

Abstract— Now-a-days many unauthorized access and theft takes place in ATM machines. In general, all the keypad based verification system has several possibilities of password guessing by way of shoulder movements and skimming device attacks. Shoulder-surfing is an attack on secret code authentication that has traditionally been hard to defeat. At the same time the growth of mobile technology, with regard to availability of services and devices like Smartphone's has created a new occurrence for message and data processing capability to do Daily Works. One such phenomenon that has emerged in the Social work Environment is BYOD (Bring Your Own Device), which means the users can use their personal device to access company resources for work [12]. This paper proposes a Wireless Pin Authentication Method (WPAM) for secure transactions using BYOD trend. In addition to that Kerberos authentication protocol is used for user's authentication. Hence, considered as a reasonable trade-off between safety, usability and cost. So, this paper mainly concentrates on providing efficient security to ATM against theft.

Keywords— Personal identification number, Skimming attack, Pin Verification, Shoulder surfing attack, Wi-Fi.

I. INTRODUCTION

Nowadays many unauthorized access, threats and theft takes place in ATM machines. Currently PIN numbers are used for security in ATMs. The crime rates are also increased with fleeting time and will never fall as attackers are efficient enough with all detailed criminal knowledge collected with them. The service provider must promote a stable security of user data for customer satisfaction. The goal is to protect ATM from theft using counter measures for security. As the ATM related security are public and published in newspaper and internet. So the security measures applied are known to both the regulator and attacker. Nowadays we use 4-Digit PIN code for safety and security for money deposition and transaction. But in real the PIN numbers can be hacked easily through specific fraudulent activities and it can be observed by human or device attackers. The attackers now are technically knowledgeable they have every idea about the usage of the user. At first, the attacker will try hacking the 4-PIN code using finger prints plated in the number box. Then the hacker tries hacking the bar code of the card using the detector and a duplicate card of the user is framed for theft. Through this method the thief can withdraw our money without the regulators knowledge and initiate theft without any doubt.

Currently Personal Identification Number (PIN) is used for security in ATMs and authentication is provided by the Users entering (PIN). This PIN numbers can be hacked easily through specific fraudulent activities and it can be observed by human or skimming device attackers. So, this paper proposes a Wireless Pin Authentication Method (WPAM) for secure ATM transaction using Wi-Fi technology. In this method, customers use their own wireless devices (Laptop, Smartphone and Tablet) for ATM Transactions.

In general, all the keypad based authentication system has several possibilities of password guessing by means of shoulder movements and skimming device attacks. The main objective of this paper is to develop a secure ATM Transaction for users using their own wireless devices (Laptop, Smartphone and Tab).

II. RELATED WORKS

Several Pin Authentication Methods are discussed as follows.

2.1. Black and White (BW) Method [1]:

The regular numeric keypad is colored at random, half of the keys in black and the other half in white, which is called as BW technique. A user who knows the correct PIN digit can answer its color by pressing the separate color key. The basic BW method is expected to resist a human shoulder surfing attack. But if the selected halves were memorized or written on a paper for m consecutive rounds and recalled to derive their Grouping Patterns, the shoulder surfer could recognize a single digit of the PIN.

2.2. Fake Cursors Method [2]:

To hide password entry on on-screen keyboards. The objective of the fake cursor is, adding overhead to the input to make it hard to monitor. The authors suggest several concurrent cursors that move in the exact same way to quickly reach objects on big screen spaces. In the past which include; chip distortion, card misplacement. Card fraud, etc. these entire problems are associated with using smartcard access control in ATM. To overcome these problems it is advisable that government should partner with banking sector to implement the use of biometric technique "intelligent voice-based access control" in ATMs, as this will eliminate completely the problems associated with smartcard access control [8, 9, 10].

2.3. Attacks on Pin Entry:

a. Shoulder Surfing Attack

In a shoulder-surfing attack (SSA), the attacker detects the logon procedure by looking over the user's shoulder, and tries to recover that user's PIN. The SSA may be done directly through the human eyes or by using any electronic devices such as fixing a skimmer device or mini cameras at ATMs [4, 6, 13].

b. Skimming Attack

A device that reads and stores magnetic stripe information when a card is swiped. Attackers can fixing a skimmer over the card slot of an ATM and store customers' credit information without their knowledge. Later, this information can be retrieved and used to make duplicates of the original cards [5, 13].

c. Eavesdropping Attack

In Eavesdropping attack, the Eavesdropper secretly listening to another person's conversation. In this attack the Eavesdropper secretly observing the users pin entry.

d. Guessing Attack

In a guessing attack, the attacker guesses a user's PIN and inputs it to pass the test. The most common type of attack is password guessing. Attackers can guess passwords locally or remotely using either a manual or robotic approach. For example, a typical ATM permits three trials [13].

III. PROPOSED SYSTEM

The main objective of this system is to develop a secure ATM. In general, all the keypad based authentication system having several possibilities of password guessing by means of shoulder movements. Shoulder-surfing is an attack on password authentication that has traditionally been hard to defeat [1]. Automated Teller Machines (ATMs) security is the field of study that aims at solutions that provide multiple points of protection against physical and electronic theft from ATMs. Authentication of users at automatic teller machines (ATMs) is mostly dependent on PIN-based verification. This paper proposes a Wireless Pin Authentication Method (WPAM) for secure ATM transaction using Wi-Fi technology. In this method, customers use their own wireless devices (Laptop, Smartphone and Tablet) for ATM Transactions. Wi-Fi is commonly called as wireless LAN, it is one of those networks in which high frequency radio waves are required for transmission of data from one place to another[15]. Wi-Fi operates on several hundred feet between two places of data transmission. This technology only works on high frequency radio signals. Otherwise, it will not work properly. Nowadays this technology is used as office or home network and in many electronic devices.

Wireless LAN or Wi-Fi is divided into three main parts on which its whole working depends and all of its applications also depend on these parts i.e. infrastructure mode, ad hoc network and mixed network[15]. Kerberos authentication protocol is used for user's authentication. It works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Kerberos protocol messages are protected against eavesdropping and Replay Attacks [14].

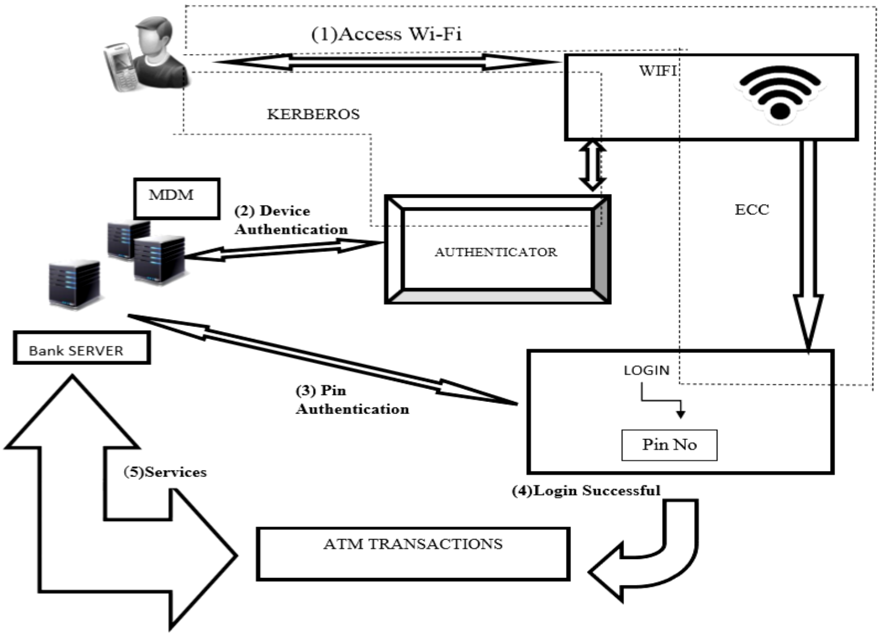


Figure 3.1-Proposed system

Steps in the proposed model:

- Registration of the user with the bank: After the registration, the wireless devices carry the public key of the user which has been signed by the bank as well as the public key of the bank.

- Optionally, the wireless device also carries an application which enables it to communicate with the ATM.
- Once that form is submitted, a unique PIN is send to the respective mail id of the user.
- Users connect the Wi-Fi enabled LAN in their Wireless Devices using the Pass code. So, Wi-Fi act as interface between wireless devices and ATM
- User authenticates himself to the wireless devices using his pin
- A wireless device authenticates itself to ATM by presenting the user's 'tickets' and responding on ATM's challenge.
- Kerberos authentication protocol is used for user's authentication[14].
- It works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.
- ATM authenticates itself to the Wireless devices by presenting its own 'tickets'. User now access the service of the ATM using the signed application.

IV. PERFORMANCE EVALUATION

4.1. BW Method

The basic BW (Black and White) method was designed to resist a human shoulder surfing attack and called the immediate oracle choices (IOC) by viewing a user as a human oracle to a system. In each round, the regular numeric keypad is colored at random in two distinct colors; half of the numeric keys in black and the other half in white.

4.2. Fingerprint Verification Method

The fingerprints of any person remains the same throughout the life and no two fingerprints are ever same. But for this to work accurately it requires clean hands without having any injuries to their prints otherwise it'll prevent proper identification

Financial bodies like banks and other organizations need to think on it and should spend extra effort and money in biometric technology and they should also endorse as a way of securing commercial transactions, across the counter and at the same instance while using the ATM.

4.3. WPAM Method

In general, all the keypad based authentication system having several possibilities of password guessing by means of shoulder movements. Shoulder-surfing is an attack on password authentication that has traditionally been hard to defeat. Automated Teller Machines (ATMs) security is the field of study that aims at solutions that provide multiple points of protection against physical and electronic theft from ATMs.

Authentication of users at automatic teller machines (ATMs) is mostly dependent on PIN-based verification. This project proposes a Wireless Pin Authentication Method (WPAM) for secure ATM transaction using Wi-Fi technology. In this method, customers use their own wireless devices (Laptop, Smartphone and Tablet) for ATM Transactions.

Wi-Fi is commonly called as wireless LAN, it is one of those networks in which high frequency radio waves are required for transmission of data from one place to another. Wi-Fi operates on several hundred feet between two places of data transmission. Kerberos authentication protocol is used for user's authentication.

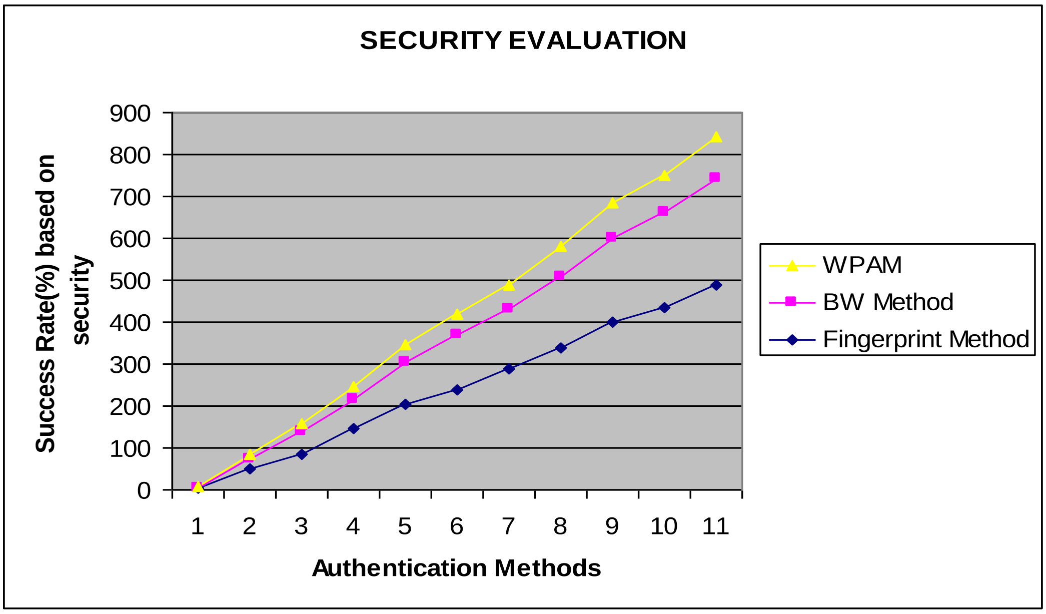


Fig. 2 Security Evaluation

V. CONCLUSION

In general, all the keypad based authentication system has several possibilities of password guessing by means of shoulder movements and skimming device attacks. Shoulder-surfing is an attack on secret code authentication that has traditionally been hard to defeat. At the Same time the growth of mobile technology, with regard to availability of services and devices like Smartphone's has created new phenomenon for message and data processing capability to do Daily Works. One such phenomenon that has emerged in the Social work Environment is BYOD (Bring Your Own Device), which means that users can use their personal device to access company resources for work [12]. This paper proposes a Wireless Pin Authentication Method (WPAM) for secure transactions using BYOD trend. In addition to that Kerberos authentication protocol is used for user's authentication.

REFERENCES

1. Taekyoung Kwon, Jin Hong, “Analysis and Improvement of a PIN-Entry Method Resilient to Shoulder-Surfing and Recording Attacks”, IEEE Transactions on Information Forensics and Security, Vol. 10, No. 2, Feb. 2015.
2. Luca, E. von Zezschwitz, L. Pichler, and H. Hussmann, “Using fake cursors to secure on-screen password entry”, In Proc. CHI, pp. 2399–2402, 2013.
3. Oyeyinka.l.K, Akinwole.A.K," Automate d Biometric Voice-Based Access Control in Automatic Teller Machine (ATM)", International Journal of Advanced Computer Science and applications, VoI.3, No.6, 2012.
4. Mun-Kyu Lee, “Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PINEntry”, In IEEE Transactions On Information Forensics And Security, VOL. 9, NO. 4, pp. 1556-6013, Apr. 2014.
5. Hong Guo, Bo Jin, “Forensic Analysis of Skimming Devices for Credit Fraud Detection”, IEEE International Conference on Information and Financial Engineering (ICIFE), pp.542 – 546, Jan. 2010.
6. V. Roth, K. Richter, And R. Freidinger, “A Pin-Entry Method Resilient Against Shoulder Surfing”, In Proc. Acm Conf. Comput. Commun Security, pp. 236– 245, Feb. 2004.
7. AbdulrahmanAlhothaily, ArwaAlrawais, Xiuzhen Cheng, RongfangBie, “A novel verification method for payment card systems”, In Springer-Verlag London, Volume 19, Issue 7, pp. 1145-1156, Oct. 2015.

8. K. Jain, A. Ross, S.Prabhakar, "An Introduction to Biometric Recognition", IEEE Trans. On Circuits and Systems for Video Technology, Vol. 14, No. 1, pp 4-19, Jan. 2004.
9. Vivek, K.Singh, Tripathi S.P, Agarwal "Formal Verification of Finger Print ATM Transaction through Real Time Constraint Notation (RTCN)", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. I May 2011.
10. Sharma, Vijay Singh Rathore,"Role of Biometric Technology over Advanced Security and Protection in Auto Teller Machine Transaction", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 - 8958, Volume-I, Issue-6, Aug. 2012
11. Zaid Imran and RafayNizami, “Advance Secure Login” International Journal of Scientific and Research Publications, Vol. 1, Issue 1, SSN 2250-3153, Dec. 2011.
12. Prashant Kumar Gajar, ArnabGhosh, ShashikantRai, "Bring Your Own Device (BYOD): Security Risks and Mitigating Strategies", Journal of Global Research in Computer Science, Volume 4, No. 4, April 2013.

Secure Data Retrieval for Decentralized Delay Tolerant Military Networks

Ms.V.Varalakshmi
Assistant Professor,
Department of Computer Science and Engineering,
St. Anne's College of Engineering and Technology.

Ms. W.Monica, Ms. T.Priyanga, Ms. S.Anugraham, Ms. H.Santhiyadevi
UG students,
Department of Computer Science and Engineering,
St. Anne's College of Engineering and Technology.

Abstract - Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Delay-tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. However, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. In this paper, we propose a secure data retrievalschemeusing CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

Keywords - Access control, attribute-based encryption (ABE), delay-tolerant network (DTN), multiauthority, secure data retrieval.

I. INTRODUCTION

In many military network scenarios, connections of wire-less devices carried by soldiers may be temporarily disconnected by jamming, environmental factors, and mobility, especially when they operate in hostile environments. Delaytolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each other in these extreme networking environments. Typically, when there is no end -to-end connection between a source and a destination pair, the messages from the source node may need to wait in the intermediate nodes for a substantial amount of time until the connection would be eventually established.

Roy and Chuah introduced storage nodes in DTN where data is stored or replicated such that onlyauthorized mobile nodes can access the necessary information quickly and efficiently.

Many military applications require increased protection of confidential data including access control methods that are cryptographically enforced in many cases, it is desirable to provide differentiated access services such that data access policies are defined over user attributes or roles, which are managed by the key authorities. For example, in a disruption-tolerant military network, a commander may store a confidential information at a storage node, which should be accessed by members of "Battalion 1" who are participating in "Region 2." In this case, it is a reasonable assumption that multiple key authorities are likely to manage their own dynamic attributes for soldiers in their deployed regions or echelons, which could be frequently changed (e.g., the attribute representing current location of moving soldiers). We refer to this DTN architecture where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN.

The concept of attribute-based encryption (ABE) is a promising approach that fulfills the requirements for se-cure data retrieval in DTNs. ABE features a mechanism that enables an access. ABE features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among private keys and ciphertexts. Especially, ciphertext-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encrypt or defines the attribute set that the decrypt or needs to possess in order to decrypt the ciphertext. Thus, different users are allowed to decrypt different pieces of data per the security policy

However, the problem of applying the ABE to DTNs introduces several security and privacy challenges. Since some users may change their associated attributes at some point (for ex- ample, moving their region), or some private keys might be compromised, key revocation (or update) for each attribute is necessary in order to make systems secure. However, this issue is even more difficult, especially in ABE systems, since each at tribute is conceivably shared by multiple users (henceforth, we bile attribute group would affect the other users in the group. For ex ample, if a user joins or leaves an attribute group, the associated attribute key should be changed and redistributed to all the other members in the same group for backward or forward secrecy. It may result in bottleneck during rekeying procedure, or security degradation due to the windows of vulnerability if the previous attribute key is not updated immediately.

Another challenge is the key escrow problem. In CP-ABE, the key authority generates private keys of users by applying the authority's master secret keys to users' associated set of at- tributes. Thus, the key authority can decrypt every ciphertext addressed to specific users by generating their attribute keys.

If the key authority is compromised by adversaries when deployed in the hostile environments, this could be a potential threat to the data confidentiality or privacy especially when the data is highly sensitive. The key escrow is an inherent problem even in the multiple-authority systems as long as each key authority has the whole privilege to generate their own attribute keys with their own master secrets. Since such a key generation mechanism based on the single master secret is the basic method mechanism based on the single master secret is the basic method attribute based or identity-based encryption protocols, removing escrow in single or multiple-authority CP-ABE is a pivotal open problem

II. EXISTING AND PROPOSED SYSTEMS

2.1. Existing System

The concept of attribute-based encryption (ABE) is a promising approach that fulfils the requirements for secure data retrieval in DTNs. ABE features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among private keys and ciphertexts. The problem of applying the ABE to DTNs introduces several security and privacy challenges. Since some users may change their associated attributes at some point (for example, moving their region), or some private keys might be compromised, key revocation (or update) for each attribute is necessary in order to make systems secure. This implies that revocation of any attribute or any single user in an attribute group would affect the other users in the group. For example, if a user joins or leaves an attribute group, the associated attribute key should be changed and redistributed to all the other members in the same group for backward or forward secrecy. It may result in bottleneck during rekeying procedure, or security degradation due to the windows of vulnerability if the previous attribute key is not updated immediately.

2.2. Disadvantages of Existing System:

- The problem of applying the ABE to DTNs introduces several security and privacy challenges. Since some users may change their associated attributes at some point (for example, moving their region), or some private keys might be compromised, key revocation (or update) for each attribute is necessary in order to make systems secure.
- However, this issue is even more difficult, especially in ABE systems, since each attribute is conceivably shared by multiple users (henceforth, we refer to such a collection of users as an attribute group)
- Another challenge is the key escrow problem. In CPABE, the key authority generates private keys of users by applying the authority’s master secret keys to users’ associated set of attributes.
- The last challenge is the coordination of attributes issued from different authorities. When multiple authorities manage and issue attributes keys to users independently with their own master secrets, it is very hard to define fine-grained access policies over attributes issued from different authorities.

2.3. Proposed System

In this section, we provide a multi authority CP-ABE scheme for secure data retrieval in decentralized DTNs. Each local authority issues partial personalized and attribute key components to a user by performing secure 2PC protocol with the central authority. Each attribute key of a user can be updated individually and immediately. Thus, the scalability and security can be enhanced in the proposed scheme. Since the first CP-ABE scheme proposed by Batten courtesan. dozens of CP-ABE schemes have been proposed. The subsequent CP-ABE schemes are mostly motivated by more rigorous security proof in the standard model.

In this model, we also use standard algorithm for key generation and we improved the security in storage node. We also provide new data access scheme which improves the security in accessing the data and also improves the data integrity.

2.4. Advantages of Proposed System:

1. **Data confidentiality:** Unauthorized users who do not have enough credentials satisfying the access policy should be deterred from accessing the plain data in the storage node. In addition, unauthorized access from the storage node or key authorities should be also prevented.
2. **Collusion-resistance:** If multiple users collude, they may be able to decrypt a cipher text by combining their attributes even if each of the users cannot decrypt the cipher text alone.

3. **Backward and forward Secrecy:**

In the context of ABE, backward secrecy means that any user who comes to hold an attribute (that satisfies the access policy) should be prevented from accessing the plaintext of the previous data exchanged before he holds the attribute. On the other hand, forward secrecy means that any user who drops an attribute should be prevented from accessing the plaintext of the subsequent data exchanged after he drops the attribute, unless the other valid attributes that he is holding satisfy the access policy.

2.5. System Architecture

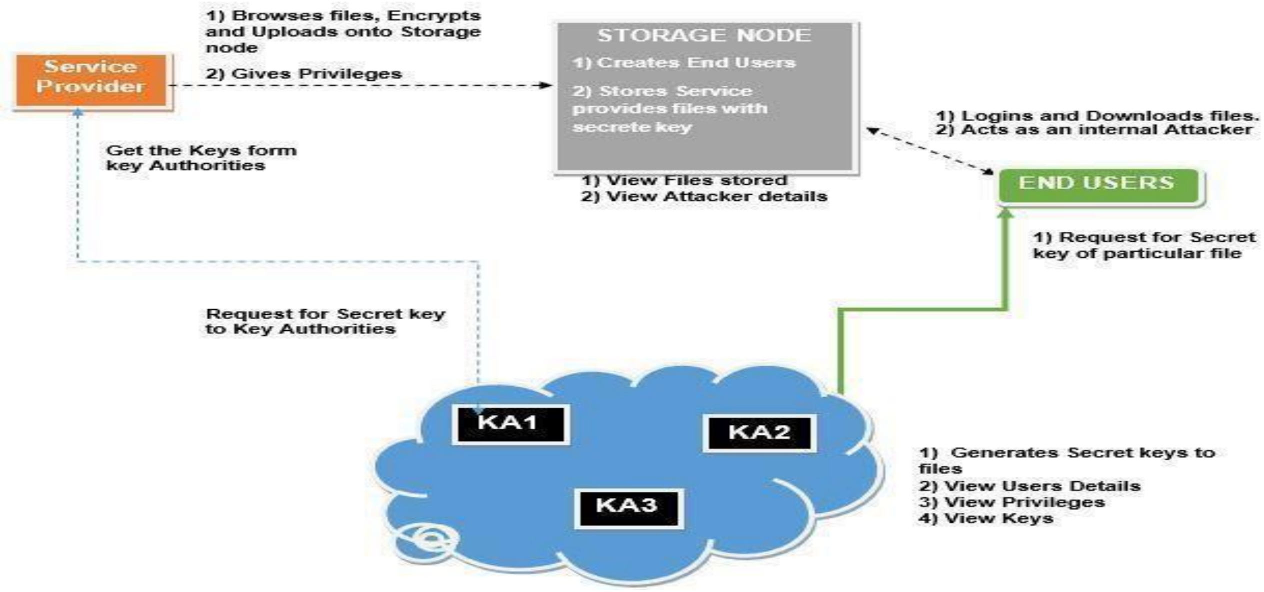

1) Browses files, Encrypts and Uploads onto Storage node
2) Gives Privileges
Service Provider
STORAGE NODE
1) Creates End Users
2) Stores Service provides files with secrete key
1) Logins and Downloads files.
2) Acts as an internal Attacker
Get the Keys form key Authorities
1) View Files stored
2) View Attacker details
END USERS
1) Request for Secret key of particular file
Request for Secret key to Key Authorities
KA1
KA2
KA3
1) Generates Secret keys to files
2) View Users Details
3) View Privileges
4) View Keys

Fig. 1. Architecture of secure data retrieval in a delay tolerant military network

2.6. System Description and Assumptions

1. Key Authorities:

They are key generation centers that generate public/secret parameters for CP-ABE. The key authorities consist of a central authority and multiple local authorities. We assume that there are secure and reliable communication channels between a central authority and each local authority during the initial key setup and generation phase. Each local authority manages different attributes and issues corresponding attribute keys to users. They grant differential access rights to individual users based on the users' attributes. The key authorities are assumed to be honest-but curious. That is, they will honestly execute the assigned tasks in the system, however they would like to learn information of encrypted contents as much as possible.

2. Storage node :

This is an entity that stores data from senders and provide corresponding access to users. It may be mobile or static. Similar to the previous schemes, we also assume the storage node to be semi trusted, that is honest-but-curious.

3. Sender :

This is an entity who owns confidential messages or data (e.g., a commander) and wishes to store them into the external data storage node for ease of sharing or for reliable delivery to users in the extreme networking environments. A sender is responsible for defining (attribute based) access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node.

4. *Soldier :*

This is a mobile node who wants to access the data stored at the storage node (e.g., a soldier). If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the sender, and is not revoked in any of the attributes, then he will be able to decrypt the ciphertext and obtain the data.

5. *CP-ABE Method :*

In Ciphertext Policy Attribute based Encryption scheme, the encryptor can fix the policy, who can decrypt the encrypted message. The policy can be formed with the help of attributes. In CP-ABE, access policy is sent along with the ciphertext. We propose a method in which the access policy need not be sent along with the ciphertext, by which we are able to preserve the privacy of the encryptor. This techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous Attribute- Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt.

III. CONCLUSION

DTN technologies are becoming successful solutions in military applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. CP-ABE is a scalable cryptographic solution to the access control and secure data retrieval issues. In this paper, we proposed an efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed even under the hostile environment where key authorities might be compromised or not fully trusted. In addition, the fine-grained key revocation can be done for each attribute group. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

REFERENCES

1. J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, “Maxprop: Routing for vehicle-based disruption tolerant networks,” in Proc. IEEE INFOCOM, 2006, pp. 1–11.
2. M. Chuah and P. Yang, “Node density-based adaptive routing scheme for disruption tolerant networks,” in Proc. IEEE MILCOM, 2006, pp. 1–6.
3. M. M. B. Tariq, M. Ammar, and E. Zequra,
4. “Mesage ferry route design for sparse ad hoc networks with mobile nodes,” in Proc. ACM MobiHoc, 2006, pp. 37–48.
5. S. Roy andM. Chuah, “Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs,” Lehigh CSE Tech. Rep., 2009.
6. M. Chuah and P. Yang, “Performanc evaluation of content-based information retrieval schemes for DTNs,” in Proc. IEEE MILCOM, 2012, pp. 1–7.
7. M. Kallahalla, E. Riedel, R. Swaminathan, Q.Wang, and K. Fu, “Plutus: Scalable secure file sharing on untrusted storage,” in Proc. Conf. File Storage Technol., 2014, pp. 29–42.
8. R. Ostrovsky, A. Sahai, and B. Waters, “Attribute-based encryption with non-monotonic access structures,” in Proc. ACM Conf. Comput. Commun. Security, 2015, pp. 195–203.

Standard Android API and Low Cost In-Vehicle Infotainment Devices

Ms. D.Anbarasi, Assistant Professor,
Department of Information Technology,
Anand Institute of Higher Technology
Mr. Logadeepan K, Mr. Rajesh S, Mr. Nelson Leo A, Mr. Madhavan A
Department of Information Technology
Anand Institute of Higher Technology

Abstract - In this modern age automotive industries are changing and updating in rapid ways as in term of engine performance and in terms of safety, economic and efficient way of transport. In this paper we are proposing an idea to build low cost car infotainment system based on android. These would help user to drive safely and efficiently. The infotainment system will run on any android phone with car specified requirement. This system will get input from various hardware and sensors like Level, Temperature, Tyre pressure, Speed Sensor with GPS and internet service ready. This system will have built in features of luxury car to mid-low range of vehicle. This system will be based on open source android with third party application support. The Application Programming Interface and the concepts proposed in this paper should reduce the closed, proprietary and non-extensible systems being released today and bolster the design and development of open, more complete, feature-full systems in vehicles that will not only assist but also entertain drivers and passengers.

Index Terms: ***Android car infotainment system, engine diagnosis, monitoring, security, GPS.***

I. INTRODUCTION

In this modern age the technology is moving fast and we have seen that any new technology introduced will be offered at high price. If we elaborate this any new technology is first introduced in high segment of car than it is used in lower segment car later on. The idea, what is been proposed is to give lower segment of car the new technology & feature at low cost. The features will include GPS navigation, accelerometer, TPMS, proximity, reverse camera, engine diagnosis, multimedia HD content, gas sensor, other device attachment, etc. Android will support all this hardware and sensor, including raw data coming from ECU. When focusing on mid range cars which covers 90 percent of population in India, the user is only given features worth his money which is analogue and manual system.

II. IN-VEHICLE INFOTAINMENT SYSTEM

IVI system such as BMW's I-drive, Audi's MMI and Alpine after market solution has been primary application platform to provide interactive automotive features till now. IVI systems are integrated into the car and provide all in one solution car infotainment and drivers friendly display and control. Most of modern In-Vehicle Infotainment (IVI) devices are based on proprietary systems. The integration of various services in infotainment devices is covered by many standards, but the support for internet, and multimedia is not available in a systematic way. Instead of building all of the aforementioned functionalities on top of the proprietary systems, integration of IVI functionality into multimedia-enabled devices could be used as an alternative approach. This approach could benefit from the rich multimedia environment already available in various devices. One such device to be integrated with IVI could be the Android device. Because of the fast evolution of electronic technologies, the automotive industry cannot adopt new technology easily. IVI platform standards were developed by automotive OEM (Original equipment manufacturer) and suppliers ,but the problem with faster adoption of new technologies still exists. Different limitations are identified in currently available IVI systems. The increasing activity in the automotive infotainment area faces a strong limitation: the slow pace at which the automotive industry is able to make vehicles "smarter". In contrast, the smartphone industry is advancing quickly. There are already several Android based applications that utilize data from the vehicle, but there is no systematic approach in utilization of that data so it can be used by any application written for that platform. The system proposed in this paper provides a standardized way of application development so development costs can be reduced, newly created applications can be easily introduced in already deployed devices, and the specific adaptions for certain systems can be done. This paper also describes the general system approach and gives component specifications along with basic operational principles of the proposed system.

III. EXISTING SYSTEM

Current IVI systems have a common feature base which includes: navigation, radio, multimedia, climate control, vehicle data monitoring and basic safety support. On-board diagnostics - is a reporting and diagnostics feature that is present in almost all vehicles on the road (with slightly different variants). The diagnostics collects and reports relevant data that can help identify problems or provide analysis of various factors. By using the standardized API, as the one proposed in this paper, and exploiting different API functionalities proposed in this paper, developers can use voice recognition to initiate air conditioning, activate window wipers and much more. This is why a standard framework needs to be designed, and followed by vehicle manufacturers. Vehicle manufacturers must expose API of the vehicle computer to allow developers to build applications that can control certain vehicle functionalities. Proposed API addresses all of the functionalities with a single, unified approach.

3.1. Disadvantages :

- Missing standardized application programming interface to develop applications for IVI devices
- Missing possibility of application distribution between different vehicle manufacturers
- Missing community for the development of IVI applications
- Missing option to upgrade IVI system (due to proprietary and closed source code)

IV. PROPOSED SYSTEM

In this paper all the parameters are measured and can be monitored from an android app using Bluetooth. Various sensors are being used to monitor the car datas such as Pressure Sensor for measuring tyre pressure, Level sensor is used to monitor the petrol level in the car tank, Speed sensor is being used to monitor the speed of the car, and Car temperature is also monitored in order to maintain a proper temperature at certain limits. Apart from this, the user will be able to see the contacts and listen the music using this app. The datas from all these parameters are passed to the controller, from where these datas will be sent to the app through Bluetooth module.

4.1. Advantages:

- Standard application environment.
- Up gradation can be done according to the car features
- Low price enables this device to use in the budget cars.

V. LITERATURE SURVEY

This system aims to provide a low-cost means of monitoring a vehicle¿s performance and tracking by communicating the obtained data to a mobile device via Bluetooth. Then the results can be viewed by the user to monitor fuel consumption and other vital vehicle electromechanical parameters. Data can also be sent to the vehicles maintenance department which may be used to detect and predict faults in the vehicle. This is done by collecting live readings from the engine control unit (ECU) utilizing the vehicle¿s built in on-board diagnostics system (OBD). An electronic hardware unit is built to carry-out the interface between the vehicle¿s OBD system and a Bluetooth module, which in part communicates with an Android-based mobile device. The mobile device is capable of transmitting data to a server using cellular internet connection.[1].

The automotive infotainment industry is currently pressured with many challenges. Tier-one manufactures must accommodate disparate and quickly changing features for different carmakers. Moreover, the use of a dedicated platform for each brand and model is no more viable. The use of an open platform would permit sharing costs across the whole customer spectrum, and it will allow products to grow and adapt to the user preferences, by providing the possibility of executing third-party applications. Google Android is a recent operating system, designed for mobile devices that perfectly fits to embedded devices such as those used for automotive infotainment. In this paper we present a proof-of-concept architecture developed in cooperation between Magneti Marelli and Politecnico di Torino, whose main contribution is an automotive-oriented extension of Google Android that provides features for combining extendibility and safety requirements.[2]

For in-vehicle infotainment systems, there are special requirements for the user interface (UI) regarding driver distraction. As a result, unlike web applications,new applications should be specifically developed for the infotainment system. Further, the user interface of the new applications should be consistent with the user interface of the main functions of the system with the result that the user can interact with the new applications as he is used to. At the same time, the applications should be compatible with different systems in order to minimize the development cost. We present an approach which allows integration of new applications into different in-vehicle infotainment systems via consumer electronics devices. While applications are deeply integrated into the user interface, development cost is minimized and still specific adaptions for certain systems are possible.[3]

Applications and networking are the key functions for connected vehicle. And applications of In-Vehicle Infotainment (IVI) system are one of the important characteristics in the automotive industry. Because of the fast evolution of electronic technologies, automotive industry cannot adopt new technology easily. IVI platform standard was developed by automotive OEM and suppliers but the problems still exist. In this paper, we propose an implementation technique of applications that are based on HTML5 and a simple way to access the mobile network. XML-based configuration is used to represent the capability of the vehicle, IVN signals of the production vehicle is used to validate the interaction between IVI system and vehicle. The application works well with native application APIs and HTML5 APIs as well as interact with vehicle and mobile network.[4]

The current technological trend in car navigation systems is toward "Display Audio" connected to a smartphone. However, there are issues with driver distraction. Therefore, we propose a new user interface for display audio. In this study, we define the requirements of a car navigation system with display audio based on the proposed new interface. We also provide a basic evaluation of this system.[5]

VI. ARCHITECTURE DIAGRAM

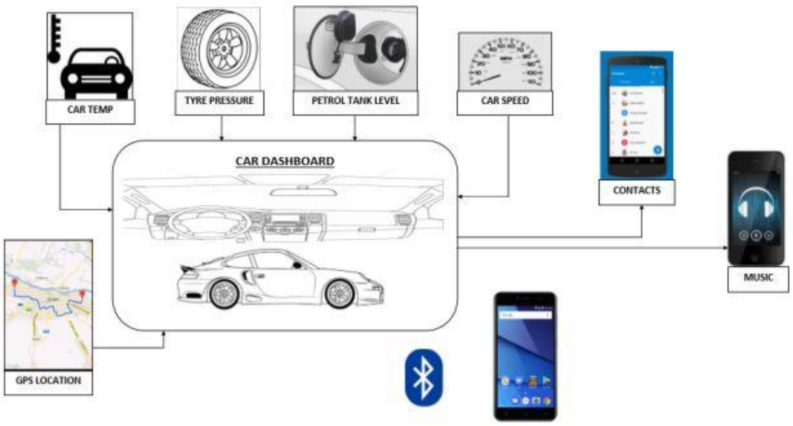


Fig 6.1 - Architecture Diagram

6.1. Hardwares Needed:

- ➢ Arduino Controller
- ➢ Level Sensor
- ➢ Pressure Sensor
- ➢ Temperature Sensor
- ➢ Speed Sensor
- ➢ GPS Module

- ➢ Voice recording Module
- ➢ Bluetooth Module

6.2. Software Needed:

- ➢ Arduino IDE
- ➢ Android studio
- ➢ Languages : Embedded C and Java

VII. HARDWARE EXPLANATION

7.1. Arduino Controller:

Arduino is an open-source project that created microcontroller-based kits for building digital devices and interactive objects that can sense and control physical devices. The project is based on microcontroller board designs, produced by several vendors, using various microcontrollers. These systems provide sets of digital and analog input/output (I/O) pins that can interface to various expansion boards (termed shields) and other circuits. The boards feature serial communication interfaces, including Universal Serial Bus (USB) on some models, for loading programs from personal computers. For programming the microcontrollers, the Arduino project provides an integrated development environment (IDE) based on a programming language named Processing, which also supports the languages C and C++. It is a microcontroller board based on the ATmega328P. It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz quartz crystal, a USB connection, a power jack, an ICSP header and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter. Arduino Uno has a number of facilities for communicating with a computer, another Arduino board, or other microcontrollers.

7.2 Level Sensor:

Level sensors detect the level of liquids and other fluids and powders that exhibit an upper free surface. Substances that flow become essentially horizontal in their containers (or other physical boundaries) because of gravity whereas most bulk solids pile at an angle of repose to a peak. There are many physical and application variables that affect the selection of the optimal level monitoring method for industrial and commercial processes. The selection criteria include the physical: phase (liquid, solid or slurry), temperature, pressure or vacuum, chemistry, dielectric constant of medium, density (specific gravity) of medium, agitation (action), acoustical or electrical noise, vibration, mechanical shock, tank or bin size and shape. Level sensors detect the level of substances that flow, including liquids, Slurries, granular materials, and powders.

7.3. Pressure Sensor:

A pressure sensor is a device which senses pressure and converts it into an analog electric signal whose magnitude depends upon the pressure applied. Pressure sensors can also be used to measure other variables such as fluid/gas flow, speed and altitude. They are also designed to measure in a dynamic mode for capturing very high speed changes in pressure. A pressure sensor measures pressure, typically of gases or liquids. Pressure is an expression of the force required to stop a fluid from expanding, and is usually stated in terms of force per unit area. A pressure sensor usually acts as a transducer; it generates a signal as a function of the pressure imposed. Pressure sensors can vary drastically in technology, design, performance, application suitability and cost. Pressure sensors that are designed to measure in a dynamic mode for capturing very high speed changes in pressure. They are used in measuring combustion pressure in an engine cylinder or in a gas turbine. These sensors are commonly manufactured out of piezoelectric materials such as quartz.

7.4. Temperature Sensor:

The LM35 series are precision integrated-circuit temperature devices with an output voltage linearly-proportional to the Centigrade temperature. The LM35 device has an advantage over linear temperature sensors calibrated in Kelvin, as the user is not required to subtract a large constant voltage from the output to obtain convenient Centigrade scaling. The LM35 device does not require any external calibration or trimming to provide typical accuracies of ±¼°C at room temperature and ±¾°C over a full −55°C to 150°C temperature range. The low-output impedance, linear output, and precise inherent calibration of the LM35 device makes interfacing to readout or control circuitry especially easy. LM35 is a precision IC temperature sensor with its output proportional to the temperature (in oC).

7.5. Speed Sensor:

Proximity Sensors using high-frequency oscillation to detect ferrous and non-ferrous metal objects and in capacitive models to detect non-metal objects. Models are available with environment resistance, heat resistance, resistance to chemicals, and resistance to water Proximity Sensors convert information on the movement or presence of an object into an electrical signal. Inductive Proximity Sensors detect magnetic loss due to eddy currents that are generated on a conductive surface by an external magnetic field. An AC magnetic field is generated on the detection coil, and changes in the impedance due to eddy currents generated on a metallic object are detected. A proximity sensor is a sensor able to detect the presence of nearby objects without any physical contact. A proximity sensor often emits an electromagnetic field and looks for changes in the field. The object being sensed is often referred to as the proximity sensor's target. The maximum distance that this sensor can detect is defined nominal range.

7.6. GPS Module:

The Global Positioning System (GPS) is a global navigation satellite system that provides location and time information in all weather conditions. The GPS operates independently of any telephonic or internet reception, though these technologies can enhance the usefulness of the GPS positioning information. GPS satellites transmit signal information to earth. This signal information is received by the GPS receiver in order to measure the user's correct position. The GPS concept is based on time and the known position of specialized satellites. GPS satellites continuously transmit their current time and position. A GPS receiver monitors multiple satellites and solves equations to determine the precise position of the receiver and its deviation from true time.

7.7. Voice recording Module:

WTV-SR is one of the members of recording serial products. WTV-SR module can record as well as fixed voice playback, recording content uploaded and a variety of control modes can be chosen. With the master chip and plug-in SPI-FLASH, it has a great advantage in the duration time of recording and cost performance. WTV-SR is provided with mp3 mode, Key control one by one, parallel interface, one-line serial interface, three-line serial interface. Therefore, WTVSR module is suit for many occasions. It can be

changed different control modes by setting I/O, which on the bottom of WTV-SR. It gives a Flexible power supply by either supply module or supply solution, so it is a effective recording solution. The recorded voice can be uploaded to the system. It also supports download voice from PC and play recorded voice with high quality. It can record up to 252 segment voice (including fixed voice) and recording time up to 1600 seconds. It supports audio recording at 10 KHz or 14
KHz sample rate.

7.8. Bluetooth Module:

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices, and building personal area networks (PANs). Invented by telecom vendor Ericsson in 1994, it was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices, overcoming problems of synchronization. Bluetooth UART enables you to wireless transmit & receive serial data. Devices equipped with Bluetooth technology support wireless point-to-point connections, as well as wireless access to mobile phones. You can simply use it for serial port replacement to establish connection between MCU and PC for data transfer. It delivers the received data and receives the data to be transmitted to and from a host system through a host controller interface.

VIII. CONCLUSION:

Thus an android application has been developed, through which an in- vehicle infotainment system can be controlled. In that the main parameters like tyre pressure, Petrol tank level, car speed and temperature along with the GPS in the android app. Along with these data the user can view the contacts and also hear the music form this system. With all the main features, this system is very feasible for the low budget cars also.

REFERENCES

1. A. Tahat, A. Said, F. Jaouni, and W. Qadamani, “Android-based universal vehicle diagnostic and tracking system,” in Proc. IEEE International Symposium on Consumer Electronics, Harrisburg, Pennsylvania, June 2012, pp. 813-819.
2. G. Macario, M. Torchiano, and M. Violante, “An in-vehicle infotainment software architecture based on google android,” in Proc. IEEE International Symposium on Industrial Embedded Systems, Lausanne, Switzerland, July 2009, pp. 257-260.
3. F. Hueger, “Platform independent applications for in-vehicle infotainment systems via integration of CE devices,” in Proc. IEEE International Conference on Consumer Electronics, Berlin, Germany, September 2012, pp. 221-222.
4. I. Son, K. Han, D. Park, M. Di Yin, and J. Cho, “A study on implementation of IVI applications for connected vehicle using HTML5,” in Proc. International Conference on IT Convergence and Security, Beijing, China, October 2014, pp. 1-4.
5. T. Yamabe, S. Ikegami, A. Ishizaki, S. Kitagami, and R. Kiyohara, “Car navigation user interface based on a smartphone,” in Proc. International Conference on Mobile Computing and Ubiquitous Networking, Singapore, January 2014, pp. 85-86.
6. N. Gandhewar and R. Sheikh, “Google Android: An emerging software platform for mobile devices,” International Journal on Computer Science and Engineering, pp. 12-17,

February 2011. [7] A. Curguz, T. Maruna, B. Kovacevic, and M. Bjelica, "Android application as parental control service in car," in Proc. Telecommunications Forum Telfor, Belgrade, Serbia, November 2015, pp. 934-937.

7. N. Puaca, M. Kovacevic, B. Kovacevic, and T. Maruna, "One solution of Android service for communication with control unit in vehicle infotainment device," in Proc. Telecommunications Forum Telfor, Belgrade, Serbia, November 2015, pp.942-945.
8. V. Cikos, M. Kovacevic, B. Kovacevic, and G. Velikic, "One solution of 3D user interface for data display on a vehicle control panel," in Proc. Telecommunications Forum Telfor, Belgrade, Serbia, November 2015, pp. 958-961.
9. B. Kovacevic, M. Kovacevic, T. Maruna, and D. Rapic, "Android4Auto: a Proposal for Integration of Android in Vehicle Infotainment Systems," in Proc. IEEE International Conference on Consumer Electronics, Las Vegas, NV, January 2016, pp.109-110.

The Dynamic Reactive Routing Protocol in VANETs

Ms. Sivasathiya.G,
Faculty,
Department of Information Technology,
Anand Institute Of Higher Technology

Ms. Nivedhitha.R, Ms. Nagalakshmi.M, Ms. Nandhini.E,
UG Students
Department of Information Technology,
Anand Institute Of Higher Technology.

Abstract*—This document explains about pure vehicle to vehicle communication in VANET. Vehicular Ad-hoc Networks (VANETs) are an emerging field, whereby vehicle-to-vehicle communications can enable many new applications such as safety and entertainment services. Most VANET applications are enabled by different routing protocols. The design of such routing protocols, however, is quite challenging due to the dynamic nature of nodes (vehicles) in VANETs. To exploit the unique characteristics of VANET nodes, in this project consists of designing a moving-zone based architecture in which vehicles collaborate with one another to form dynamic moving zones so as to facilitate information dissemination. The proposed system of this project by moving object modeling and indexing techniques from the theory of large moving object databases into the design of VANET routing protocols. The results are compared with existing state of art approaches in terms of packet delivery ratio and throughput with clustering and non-clustering approaches.

***Index Terms* - Routing protocols, Moving–zone based architecture, Modeling and indexing technique.**

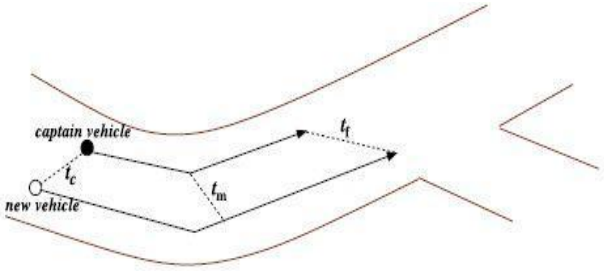
I. INTRODUCTION

This paper is based on VEHICULAR Ad-hoc Networks (VANETs) which enable vehicles to communicate with one another and create a large network with vehicles acting as the network nodes. Considering the huge number of vehicles (hundreds of millions worldwide on the road on a daily basis), the benefits of VANETs would be tremendous. Various types of information (e.g., traffic conditions, advertising news and e-coupons) can be shared between vehicles via VANETs as long as minor delays are acceptable in the specific applications of interest. For example, a vehicle can send inquiries to vehicles around certain landmarks to obtain up-to-date parking information. Another interesting emerging application, called Infotainment, provides multimedia services to subscribed vehicles in a particular location by using vehicle-to-vehicle (V2V) communication. A key requirement for the realization of VANET applications is the availability of efficient and effective routing protocols for message dissemination. Without well-defined and efficient routing protocols, vehicles may be unable to share important messages and enjoy the benefits of the advanced technologies offered by VANETs. To address these issues, many VANET routing protocols have been proposed.s are not prescribed, although the various table text styles are provided. The formatter will need to create these components, incorporating the applicable criteria that follow.

II. EXISTING SYSTEM

A key requirement for the realization of VANET applications is the availability of efficient and effective routing protocols for message dissemination. Without well-defined and efficient routing protocols, vehicles may be unable to share important messages and enjoy the benefits of the advanced technologies offered by VANETs. To address these issues, many VANET routing protocols have been proposed. Broadly, these existing protocols can be classified into five main categories, namely broadcasting protocols , route-discovery protocols, position-based protocols, clustering-based protocols and infrastructure-based protocols. While effective for specific applications and contexts, these protocols are still limited in their applicability and practical use. The broadcasting protocols rely on large message dissemination, and hence may cause a high communication overhead and message congestion on the network. To prevent this, broadcast storm mitigation techniques have been proposed. The route-discovery protocols require to discover a route be for sending out a message, and hence may not be suitable for applications with strict time constraints.

2.1. Data Diagram of Existing Models:



2.2. Limitations of Existing Models:

(i) Clusters are formed based on partitioning of road networks instead of object mobility, which reduces the lifetime of clusters.

(ii) Clustering process requires each vehicle to periodically broadcast messages or has complicated voting mechanism, which can incur high communication overhead.

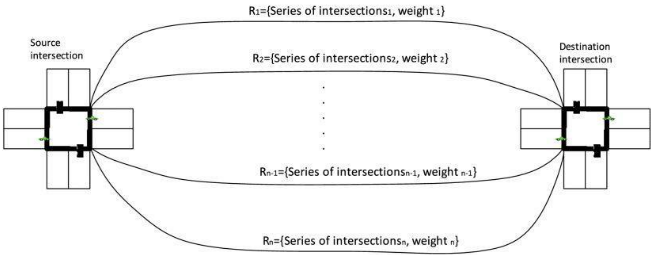
(iii) Clustering needs assistance of road-side units which may not be available in many environments.

(iv) Clustering focuses on small-scale scenarios (e.g., hundreds of vehicles).

Our proposed research will overcome these limitations.

III. PROPOSED SYSTEM

This project, proposes a comprehensive routing solution that delivers messages in VANETs via a self-organized moving-zone based using pure vehicle-to-vehicle communication. The results are compared for routing protocol with both clustering-based approaches and non-clustering based approaches to demonstrate the advantages of our approach. Our approach integrates moving object modeling and indexing techniques to vehicle management. Moving object techniques allow us to provide a realistic cluster-based representation, in that vehicles are grouped together according to their actual moving patterns.


R_1={Series of intersections$_1$, weight $_1$}
Source intersection
Destination intersection
R_2={Series of intersections$_2$, weight $_2$}
R_{n-1}={Series of intersections$_{n-1}$, weight $_{n-1}$}
R_n={Series of intersections$_n$, weight $_n$}

IV. IMPLEMENTATION

In the proposed architecture shows the RSUs an additional role in the proposed privacy framework, where they will work together and with the TA to distribute pseudonyms to passing vehicles. We are not the first to propose the use of RSUs to assist in privacy preservation in VANETs, as several frameworks have exploited this aspect to use them for distribution of pseudonyms, keys, and tokens. The number of pseudonyms available for use is directly related to the privacy achieved since a larger number allows for a higher frequency of pseudonym changing and hence more privacy. The RSUs, on the other hand, have a larger amount of resources, specifically storage capacity, and can hold a huge number of pseudonyms as compared to OBUs.

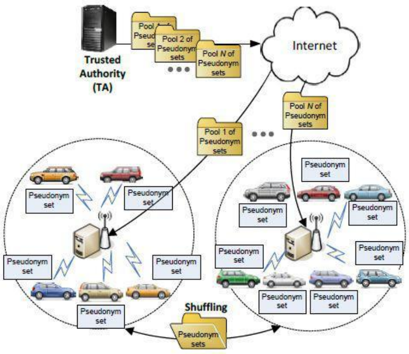


Fig. 4.1 - System Architecture

4.1. Vehicles Registration:

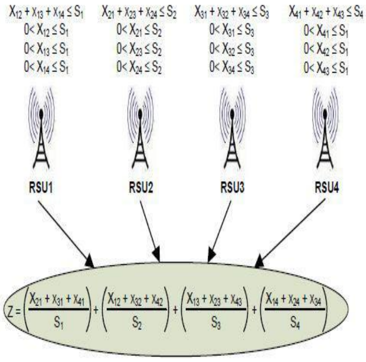
In this module the vehicles are registered if it's entered first time. Travelling Agent is aware of the existence of all RSUs and has a communication link with them. Hence, it is responsible for the generation of the pool of pseudonyms to be used by all vehicles and for the management of their distribution across the RSUs, which in turn manage the allocation of the pseudonyms to the vehicles. To achieve this, a car needs to announce the upcoming SCH that it is going to switch to. This opens the door for privacy violations, as it would allow an eavesdropping attacker to link conversing cars together, and also learn about their interests, given that a car's next service channel is a clear indicator of its interests. This issue is worsened by the fact that such information is transmitted as routine "HELLO" messages periodically during the CCH. Additionally, due to the wireless nature of VANETs, all messages sent by a car are heard by other nodes that are within its transmission range.

4.2. Generating address for vehicles:

Similar to other networked hosts, a vehicle uses two addresses: the MAC address, which is a 48-bit address that uniquely identifies a node at the link layer, and the 128-bit IPv6 address that is used for communications within the network. Hence, using one fake address on one layer of the protocol stack is not sufficient as messages with the same address at the other layers can be linked to the same vehicle. Cryptographically generated addresses (CGAs) are IPv6 addresses generated by computing a hash function using public key and additional parameters. The OBU then generates a set of pseudonyms together with appropriate certificates. Those addresses are then distributed to the vehicles through the RSUs. The CGA algorithm uses a 128-bit random number and a public key to generate the interface identifier which is then concatenated with a subnet prefix to form the IPv6 address.

4.3. Captain Vehicle Management:

This pseudonym will be used by the car to communicate with the first RSU and request a set of pseudonyms. The TA then sends the public keys of all registered cars to all the RSUs to be used for authenticating the cars, as we describe later. After generating *N* pseudonyms, the TA distributes the pseudonym sets to the RSUs, where the number of sets given to an RSU is determined based on the density of traffic surrounding it. Hence, during registration, the RSU informs the TA of the average flow rate λ of cars in its locations which is assumed to be known and determined by traffic engineers. Obviously, an RSU with a higher traffic flow rate is given a larger pool of pseudonyms than RSUs with lower λ .When the RSU receives the pool, it updates its POOLSIZE value which indicates its needs at the moment. However, this value might not be reflective of the number of cars the RSU is servicing at all times. For this, the RSU monitors λ by counting the number of pseudonym requests it is receiving per hour.


$X_{12}+X_{13}+X_{14} \le S_1$
$0 < X_{12} \le S_1$
$0 < X_{13} \le S_1$
$0 < X_{14} \le S_1$
$X_{21}+X_{23}+X_{24} \le S_2$
$0 < X_{21} \le S_2$
$0 < X_{23} \le S_2$
$0 < X_{24} \le S_2$
$X_{31}+X_{32}+X_{34} \le S_3$
$0 < X_{31} \le S_3$
$0 < X_{32} \le S_3$
$0 < X_{34} \le S_3$
$X_{41}+X_{42}+X_{43} \le S_4$
$0 < X_{41} \le S_1$
$0 < X_{42} \le S_1$
$0 < X_{43} \le S_1$
RSU1
RSU2
RSU3
RSU4
$Z=\left(\frac{X_{21}+X_{31}+X_{41}}{S_1}\right)+\left(\frac{X_{12}+X_{32}+X_{42}}{S_2}\right)+\left(\frac{X_{13}+X_{23}+X_{43}}{S_3}\right)+\left(\frac{X_{14}+X_{24}+X_{34}}{S_4}\right)$

4.4. Performance Evaluation

The performance of the network can be evaluated through (1) System Effectives, (2) Overhead, (3) Throughput.

1. **System Effectiveness:** To evaluate the efficiency of our system, we simulate a scenario using the network simulator ns2 that comprises a 10 km highway, with RSU's placed 500 m apart (consistent with rates). More specifically, the figure shows how higher car arrival rates increasingly offset the low communication activity in the network, which is justifiable since the total number of communicating vehicles, which may be approximated by the product of the arrival rate and the activity level.
2. **Overhead:** The main variables affecting the amount of overhead are the average car speed and the wireless transmission speed, as they both determine how often cars cross the boundaries of the RSU transmission ranges, thus triggering distribution of pseudonym sets and increasing the frequency of shuffling. The growth of wireless overhead traffic per RSU in response to increasing both the average car speed and the wireless transmission range of cars.
3. **Throughput:** The throughput can be measured by the simulations by choosing a random vehicle as a target and calculate the anonymity set to be the number of vehicles that change pseudonyms simultaneously with the tracked vehicle. We divide our results to scenarios where vehicles use only one pseudonym at a time and other scenarios where vehicles are allowed the simultaneous use of multiple pseudonyms for each active session.

V. RESULT AND ANALYSIS

The detailed analysis of results of simulation study has been described. The analysis of AODV and MOZO routing protocols have been performing on the basis of different performance metrics such as end to end delay and throughput with varying number of nodes.

5.1 Introduction:

This chapter present a performance analysis and improvement of AODV routing protocols for Vehicular Ad hoc Network. Both protocols were simulated using Riverbed and were compared in terms of throughput and end to end delay with varying number of mobile nodes or vehicle node densities.

5.2 Simulation Setup:

This dissertation work using a simulation tool **Riverbed**' for performing simulation. A campus network of size 1500 m x 1500 m is using for simulating varying number of mobile nodes. The all mobile nodes are spreading within this area. Each scenario takes 1200 seconds (simulation time) for running. Under each simulation we check the behaviour of AODV routing protocol with 10 m/s speed and constant (200) pause time. For examining average statistics of the network load, delay and throughput for the AODV routing protocol of VANET we collected DES (global discrete event statistics) on each protocol and Wireless LAN.

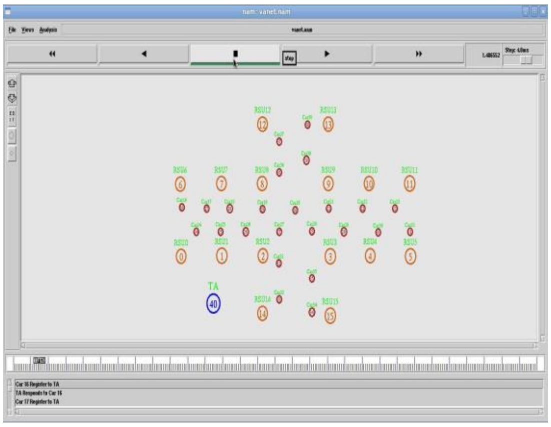
5.3 Results and Analysis:

There are various kinds of performance metrics for the performance evaluation of the routing protocols such as delay, throughput. These performance metrics arevery necessary for evaluation of the routing protocols in a communication network. In this dissertation work for performance evaluation and improvement of AODV in terms of three performance metrics such as delay and throughput. These protocols need to be checked against certain parameters for their performance. If a routing protocol gives low end to end delay so this means routing protocol is efficient as compare to the protocol which gives higher end to end delay. Similarly if a routing protocol has low network load is called as the efficient routing protocol. The same is the case with the throughput as it represents the successful deliveries of packets in time. If a protocol shows the high throughput so this means it is the best and efficient protocol rather than the routing protocol which have low throughput. These parameters have great influence in the selection of an efficient routing protocol in any communication network. In the next subsections all considered performance metrics with simulation results has been described.

5.3.1. Throughput:

Throughput can be defined as the ratio of the total amount of data reaches a destination from the source. The time it takes by the destination to receive the last message is called as throughput. It can express as bytes or bits per seconds (byte/sec or bit/sec). There are some factors that affect the throughput such as; changes in topology, availability of limited bandwidth, unreliable communication between nodes and limited energy. A high throughput is absolute choice in every network.

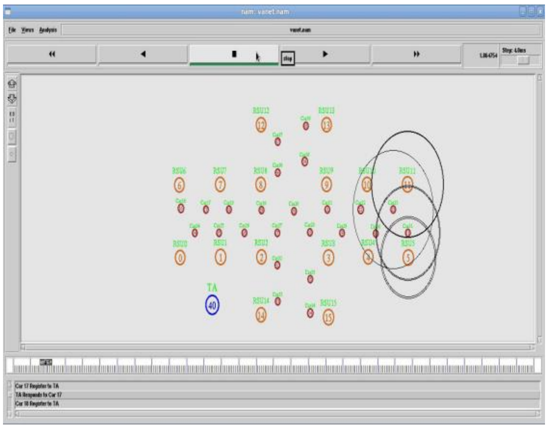
VANET FORMATION:



```
Car 16 Register to TA
TA Responds to Car 16
Car 17 Register to TA
```

This figure shows the Vehicular Network Formation consists of Travelling Agent, Road Side Units, and vehicles are moved in roads for starts communication.

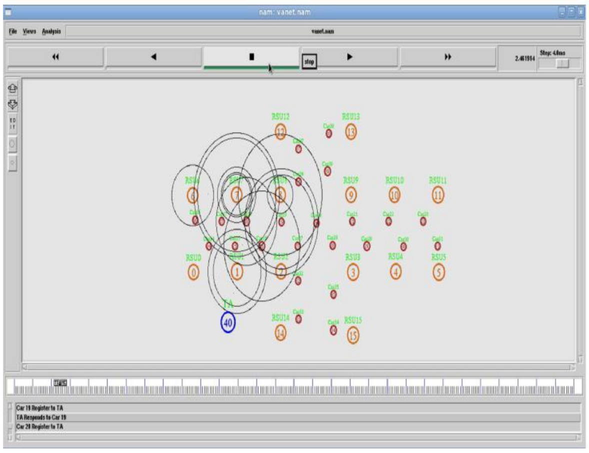
VEHICULAR TRANSMISSION:



```
Car 17 Register to TA
TA Responds to Car 17
Car 18 Register to TA
```

This figure shows the message transmission among road side units and vehicles to transmit packets from source to destination.

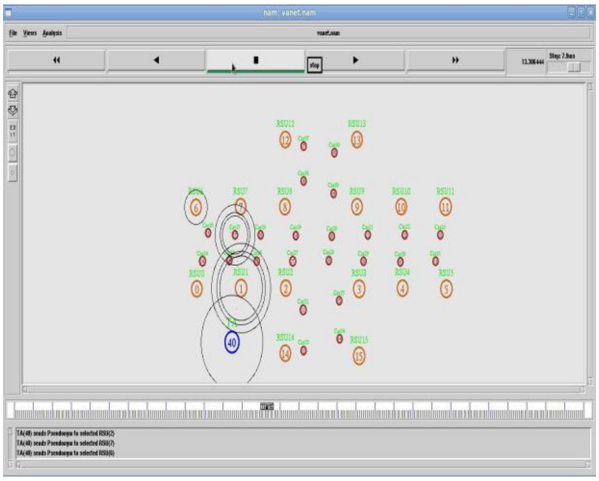
VEHICLES TRANSMITS TO ROAD SIDE UNIT:



```
Car 19 Register to TA
TA Responds to Car 19
Car 20 Register to TA
```

This figure shows when the new vehicle enters to transmission area first it's registered into travelling agent and once its registered added into

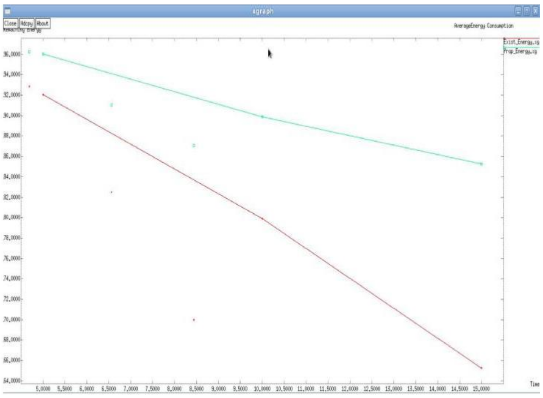
Captain Vehicle Management:



```
T.A(40) sends Pseudonym to selected RSU(2)
T.A(40) sends Pseudonym to selected RSU(7)
T.A(40) sends Pseudonym to selected RSU(6)
```

This figure represents the pseudonym transmission between the registered vehicles and the Transmitting agent.

Energy Consumption:



This figure represents the energy conversation ranges between proposed VT and DSR approach and VT saves more energy.

Packet Delivery Ratio:

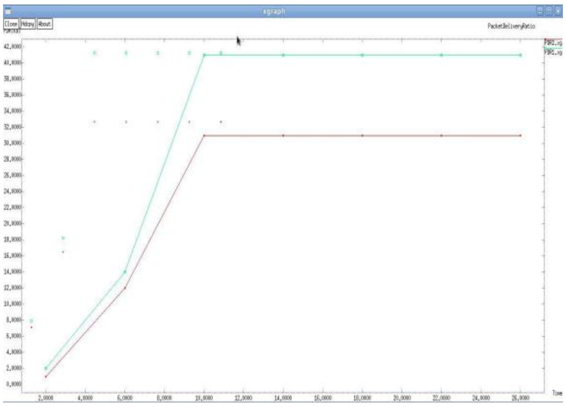
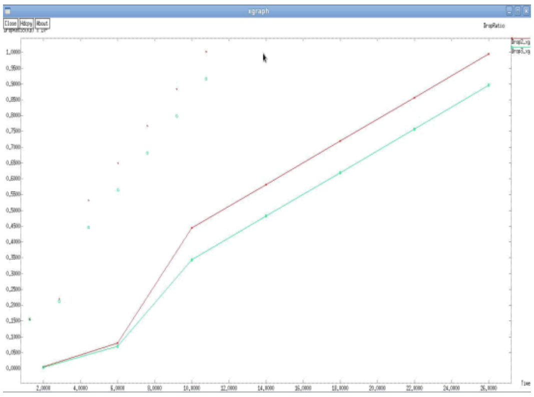


Figure represents the packet delivery ratio between proposed VT and DSR approach and VT sends more number of packets with respective to time.

Packet Drop Ratio:



This figure represents the packet drop ratio between proposed VT and DSR approach and VT shows less number of packet drops.

VI. CONCLUSION

This proposed work consists of an anonymity framework for vehicular ad hoc networks based on the use of pseudonyms. The framework comprises as main elements a Trusted Authority, the Road Side Units (RSUs), and the vehicles themselves. We introduced an innovative pseudonym management system that distributes pseudonym sets to vehicles in response to particular events that depend on vehicle speeds and how distant the RSUs are from each other. Our performance results show the ability of the system to maintain a sufficiently large anonymity set that is meant to confuse the attacker.

REFERENCES

1. Dan Lin, Jian Kang, Anna Squicciarini, Yingjie Wu, Sashi Gurung, and Ozan Tonguz, "MoZo: A Moving Zone Based Routing Protocol Using Pure V2V Communication in VANETs", in Proc. IEEE Transactions on mobile computing, VOL. 16, NO. 5, MAY 2017
2. O. K. Tonguz, N. Wisitpongphan, F. Bai, P. Mudalige, and V. Sadekar, "Broadcasting in VANET," in Proc. IEEE Mobile Netw. Veh. Environments, 2007, pp. 7–12
3. V. Naumov and T. Gross, "Connectivity-aware routing (CAR) in vehicular ad-hoc networks," in Proc. 26th IEEE Int. Conf. Comput. Commun., 2007, pp. 1919–1927
4. W. Viriyasitavat, O. K. Tonguz, and F. Bai, "UV-CAST: An urban vehicular broadcast communication protocol," IEEE Commun. Mag., vol. 49, no. 11, pp. 116–124, Nov. 2011
5. O. K. Tonguz, N. Wisitpongphan, and F. Bai, "DV-CAST: A distributed vehicular broadcast protocol for vehicular ad hoc networks," IEEE Wireless Commun., vol. 17, no. 2, pp. 47–57, Apr. 2010.
6. P. Samar, M. R. Pearlman, and Z. J. Haas, "Independent zone routing: An adaptive hybrid routing framework for ad hoc wireless networks," IEEE/ACM Trans. Netw., vol. 12, no. 4, pp. 595–608, Aug. 2004
7. C. Lochert, M. Mauve, H. Fussler, and H. Hartenstein, "Geographic routing in city scenarios," ACM SIGMOBILE Mobile Comput. Commun. Rev., vol. 9, no. 1, pp. 69–72, 2005.

Symmetric Algorithm Based Multi Secret Sharing Visual Cryptography Method for Image Processing

M.Kaviya, P.Nanthini, B.Saranya
PG Students
MRK Institute of Technology , Kattumannarkoil

Mr.R.Vijayabharathi
Assistant Professor,
Department of Computer Science and Engineering,
MRK Institute of Technology , Kattumannarkoil.

Abstract—An image can be splitted into two random shares which once individually viewed reveals no idea about the secret picture. The secret image can be obtained by union of the two shares. This method is known as Visual Cryptography. Conventional k out of n visual cryptography scheme is used to encrypt a solitary picture into n shares. The image can be decoded by using only k or more shares. Many existing illustration cryptographic methods uses binary images only for this process. This doesn't suits well for many applications. The main objective of this project is to establish message among the sender and the receiver by using emails and other communicating modes. In this work, an XOR based multi secret sharing is proposed to send images from the source to the destination in a secured way. This method eliminates the fundamental safety challenges of VC which is similar to secondary use of code book, random split patterns, expansion of pixels in collective and enhanced images, lossy recovery of secret images and limitation on number of shares. The proposed method is n out of n multi secret sharing method. Broadcast of several secret images at the same time is accomplished through this planned project. The secret picture can be uncovered only when each and every one of the n shares are accepted by the receiver and decrypted. Master share is formed at time of encryption by using a secret key and can be regenerated by using the same secret key at the instance of decryption. Experimental results show that the pixel standards of the secret images received at the destination is very elevated when compared to the available methodologies.

Index Terms — ***XOR Algorithm, Visual Cryptography, Multi Secret Sharing, Secured Communication, Pixel Expansion***

I. INTRODUCTION

Cryptography entails creating written or generated codes that enables know-how to be kept secret. Cryptography converts secret data right into a format with the intention of a beyond the understanding format for an illicit person, allowing it to be transmitted without any person decoding it back into a readable layout, as a consequence compromising the secured data. Knowledge security uses cryptography on a combination of levels. The proficiency can't be learned and a key should be used to decrypt it. The acquaintance maintains the integrity at the course of transit and while being stored. Cryptography additionally aids in non-repudiation. This means both the creator and the beneficiary of the expertise could claim they did not generate or attain it. Cryptography is popularly known as cryptology. Cryptography deals with the respectable achieving of digital data. It refers again to the intend of method founded on mathematical algorithms that afford principal capabilities security picks. The artwork and science of breaking the cipher textual content is known as cryptanalysis. The cryptographic approach effect will likely be within the cipher textual content material for conversation or storage motive. It entails the purpose of cryptographic method so as to wreck them. Cryptanalysis can be used throughout the design of the novel cryptographic techniques to scan their safety strengths. Cryptography concerns with the design of cryptosystems, while cryptanalysis studies the breaking of cryptosystems.

1.1 Types of Cryptography

1.1.1 Text Cryptography

Plain Text

In cryptography, plaintext or clear text is unencrypted information for storage or transmission. Clear text usually refers to data that is transmitted or stored unencrypted.

Cipher Text

In cryptography, cipher text is the result of encryption performed on plaintext using an algorithm. Cipher text is also known as encrypted or encoded information because it contains a form of the original plaintext that is unreadable by a human or computer without the proper cipher to decrypt it. Decryption, the inverse of encryption, is the process of turning cipher text into readable plaintext.

1.1.2 Image Cryptography

Visual Cryptography is a cryptographic manner which makes it possible for photographs to be encrypted in this kind of approach that decryption becomes the job of the character to decrypt by way of sight studying. A visible secret sharing scheme is a method, the place an snapshot was once damaged up into n shares in order that best anybody with all n shares could decrypt the photograph, while any n − 1 shares printed no understanding concerning the original photo. Each share was once printed on a separate transparency, and decryption used to be performed by means of protecting the shares. When all n shares were overlaid, the fashioned picture would show up.

1.2 Types of Cryptosystems

Fundamentally, there are two types of cryptosystems based on the manner in which encryption - decryption is carried out in the system:

- Symmetric Key Encryption
- Asymmetric Key Encryption

The main difference between these cryptosystems is the relationship between the encryption and the decryption key. Logically, in any cryptosystem, both the keys are closely associated. It is practically impossible to decrypt the cipher text with the key that is unrelated to the encryption key.

1.2.1 Symmetric Key Encryption

The encryption process where same keys are used for encrypting and decrypting the information is known as Symmetric Key Encryption. The study of symmetric cryptosystems is referred to as symmetric cryptography. Symmetric cryptosystems are also sometimes referred to as secret key cryptosystems. A few well-known examples of symmetric key encryption methods are: Digital Encryption Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.

The salient features of cryptosystem based on symmetric key encryption are:

- Persons using symmetric key encryption must share a common key prior to exchange of information.
- Keys are recommended to be changed regularly to prevent any attack on the system.
- A robust mechanism needs to exist to exchange the key between the communicating parties. As keys are required to be changed regularly, this mechanism becomes expensive and cumbersome.
- In a group of n people, to enable two-party communication between any two persons, the number of keys required for group is n × (n – 1)/2.

- Length of Key (number of bits) in this encryption is smaller and hence, process of encryption - decryption is faster than asymmetric key encryption.
- Processing power of computer system required to run symmetric algorithm is less.

1.2.2 Asymmetric Key Encryption

The encryption process where different keys are used for encrypting and decrypting the information is known as Asymmetric Key Encryption. Though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting cipher text is feasible. Asymmetric Key Encryption are pre-shared secret key between communicating persons.

The salient features of this encryption scheme are as follows:

- Every user in this system needs to have a pair of dissimilar keys, private key and public key. These keys are mathematically related – when one key is used for encryption, the other can decrypt the cipher text back to the original plaintext.
- It requires putting the public key in public repository and the private key as a well guarded secret. Hence, this scheme of encryption is also called Public Key Encryption.
- Though public and private keys of the user are related, it is computationally not feasible to find one from another. This is strength of this scheme.
- When sender needs to send data to receiver, the public key of receiver is received from repository, encrypts the data and transmits.
- Receiver uses the private key to extract the plaintext.
- Length of Keys (number of bits) in this encryption is large and hence, the process of encryption-decryption is slower than symmetric key encryption.
-
- Processing power of computer system required to run asymmetric algorithm is higher.

1.3 Security Services of Cryptography

The primary objective of using cryptography is to provide the following four fundamental information security services

Confidentiality

Confidentiality is the most important protection carrier furnished by way of cryptography. It is a protection carrier that maintains the information from an unauthorized man or woman. It is routinely referred to as privacy or secrecy. Confidentiality can be finished through numerous manner commencing from physical securing to the use of mathematical algorithms for information encryption.

Data Integrity

It is safety service that deals with deciding upon any alteration to the information. The data could get modified with the aid of an unauthorized entity intentionally or accidently. Integrity provider confirms that whether or not knowledge is undamaged or no longer since it was once last created, transmitted or saved via a certified person. Data integrity can not restrict the alteration of knowledge, but presents a way for detecting whether data has been manipulated in an unauthorized manner.

Authentication

Authentication provides the identification of the originator. It confirms to the receiver that the data received has been sent only by an identified and verified sender. Authentication service has two variants:

- **Message authentication** identifies the originator of the message without any regard router or system that has sent the message.
- **Entity authentication** is assurance that data has been received from a specific entity, say a particular website.

Apart from the originator, authentication may also provide assurance about other parameters related to data such as the date and time of creation/transmission.

Non-repudiation

It is a protection carrier that ensures that an entity are not able to refuse the ownership of a prior commitment or an action. It's an assurance that the long-established creator of the info cannot deny the creation or transmission of the mentioned knowledge to a recipient or others. Non-repudiation is a property that is most fascinating in circumstances the place there are possibilities of a dispute over the exchange of knowledge.

The rest of this paper is organized as follows: Section 2 is about the related work about visual cryptography. Section 3 deals with the existing method. Section 4 explains the proposed method. Section 5 is performance evaluation.

II. RELATED WORK

In [1] G. Ateniese et.al., proposes an extended visual cryptography scheme (EVCS), a technique to encode images, for an access structure (ΓQual; ΓForb) on a set of n participants, in such a way that when stack together the transparencies associated to participants in any set X € ΓQual, we get the secret message with no trace of the original images, but any X € ΓForb has no information on the shared image. Moreover, after the original images are encoded they are still meaningful.(ie) any user will recognize the image on his transparency.

In [2] A. Beimel et.al., shows that any information inequality with four or five variables cannot prove a lower bound of ω (n) on the share size. In addition, it is shown that the same negative result holds for all information inequalities with more than five variables that are known to date.

In [3] M. Bose et.al., employed a Kronecker algebra to obtain necessary and sufficient conditions for the existence of a (k, n) VCS with a prior specification of relative contrasts that quantify the clarity of the recovered image. Also showed how block designs can be used to construct VCS which achieve optimality with respect to the average and minimum relative contrasts but require much smaller pixel expansions than the existing ones.

In [4] O. Farras et.al., proposed the search of bounds on the information ratio of non-perfect secret sharing schemes. This work extends the known connections between polymatroids and perfect secret sharing schemes to the non-perfect case. Proved that there exists a secret sharing scheme for every access function. Uniform access functions, that is, the ones whose values depend only on the number of participants, generalize the threshold access structures.

In [5] M. Sasaki et.al., provides a formulation of encryption for multiple secret images, which is a generalization of the existing ones and also a general method of constructing VSS schemes encrypting multiple secret images.

In [6] S. Washio et.al., examines the security of an audio secret sharing scheme encrypting audio secrets with bounded shares and optimizes the security with respect to the probability distribution used in its encryption.

In [7] Kai-Hui Lee et.al., proposes an algorithm that adopts a novel hybrid encryption approach that includes a VC-based encryption and a camouflaging process. The experimental results demonstrate that the proposed approach not only can increase the capacity efficient for VSSM schemes, but also maintains an excellent level of contrast in the recovered secret images.

In [8] Y. C. Chen et.al., proposes a new notion of non-monotonic visual cryptography (NVC) for human vision system as a primitive to construct FIVC. Presents an ideal construction of simple NVC which relies on a slightly unreasonable assumption. Based on the simple NVC, shows a few methods to extend the functionality for complicated cases of NVC. Then, the generic construction is presented as a systematic manner to eliminate the above assumption. Finally, formally introduce a transformation NVC-to-FIVC algorithm which takes NVC as input and then produce a construction of FIVC. Also, show a demonstration the NVC-to-RIVC algorithm and analyze some properties regarding NVC.

In [9] C.N. Yang et.al., considers the case when the secret image is more than one and this is a so-called multi-secret VCS (MVCS). Also discusses a general (k, n)-MVCS for any k and n. This paper has three main contributions: (1) this scheme is the first general (k, n)-MVCS, which can be applied on any k and n, (2) gives the formal security and contrast conditions of (k, n)-MVCS and (3) theoretically prove that the proposed (k, n)-MVCS satisfies the security and contrast conditions.

In [10] S. J. Shyu et.al., presents a formal definition to (k, n)-VCS-MS and develops an efficient construction by way of integer linear programming. Experimental results demonstrate the effectiveness of the construction.

III. EXISTING SYSTEM

In the existing method, the variety of the access control of visual secret sharing (VSS) schemes encrypting a couple of photographs is maximized. First, the formulation of entry structures for a single secret's generalized to that for a couple of secrets. This generalization is maximal in the sense that the generalized system makes no restrictions on access buildings; in unique, it entails the prevailing ones as distinctive circumstances. Subsequent, a ample to be satisfied via the encryption of VSS schemes realizing an entry structure for a couple of secrets of essentially the most general type is offered, and two constructions of VSS schemes with encryption pleasing this are supplied. Every of the two constructions has its expertise in opposition to the opposite; one is extra general and may generate VSS schemes with strictly better distinction and pixel growth than the opposite, while the opposite has an easy implementation. Additionally, for threshold entry buildings, the pixel expansions of VSS schemes generated through the latter building are estimated and become the same as these of the prevailing schemes known as the brink a couple of secret visible cryptographic schemes (MVCS). In the end, the optimality of the previous construction is examined, giving that there exist entry constructions for which it generates no most suitable VSS schemes

IV. PROPOSED SYSTEM

The main objective of this project is to launch secured image transfer between the source and the destination through e - mails and supplementary communicating modes. In this project, users should register with the server to exchange images within themselves. All users should be genuine during the time of registration. An email will be sent to the registered mail. The mail contains a onetime password. The user has to enter it to activate the account. Then only the user is permitted to communicate with other users. An XOR based method using multi secret sharing is implemented to send images from the source to the destination using a secured way. The proposed system eliminates the major safeguard features of VC like exterior use of code book, random share patterns, expansion of pixels in shared and recovered images, lossy recovery of secret images and limitation on number of shares. The proposed method is an n out of n multi secret sharing scheme. Communication of multiple secret shares simultaneously is achieved through this proposed method. The private key will sent to the receiver through mobile. Using that only, the decryption is possible. The secret image can be exposed only when all the n shares are received by the receiver and decrypted. Tentative results show that the pixel values of the secret images received at the destination is very high when compared to the existing methodologies.

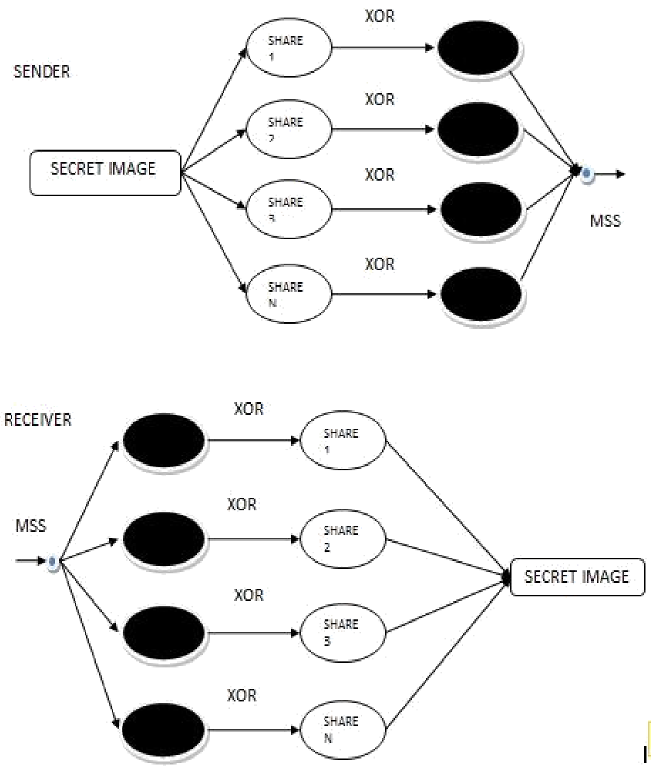


Figure 4.1- System Architecture of the proposed system

V. PERFORMANCE EVALUATION

To demonstrate the efficiency and feasibility of the proposed XOR based multi-secret sharing scheme, the encrypting/decrypting experiments are conducted on various set images.

A & B are original images. The original images are splitted using rows and columns. C & D are the first shares of A & B respectively. Like this numerous shares will be formed based on rows and columns. E & F are the encrypted shares of C & D. G & H are the decrypted shares of E & F. I
& J are the recovered images. XOR algorithm is used for encryption and decryption.

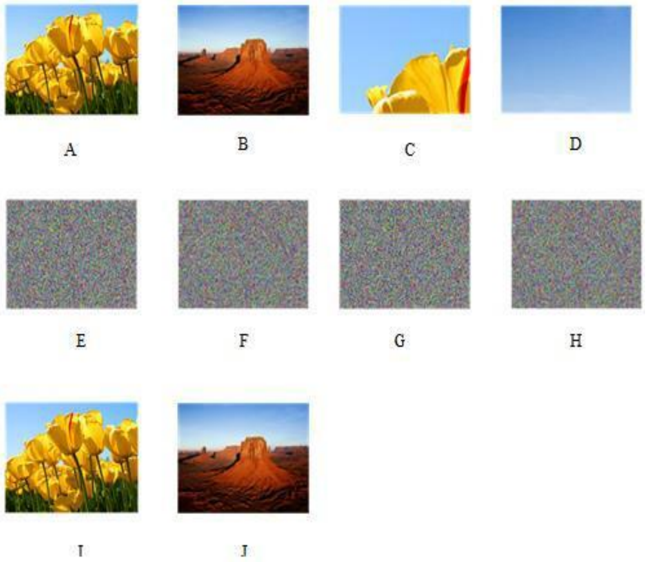


Fig : 2 : Experimental Results for n=2 : A- Sen$_1$, B – Sen$_2$, C- Sha$_1$, D – Sha$_2$, E - Enc$_1$ F- Enc$_2$ G – Dec$_1$ H – Dec$_2$ I – Rec$_1$ J – Rec$_2$

$$\text{MSE} = \frac{1}{}\sum_{=0}^{-1}\sum_{=0}^{-1}((\ (\ ,\ ) - \ (\ ,\ ))^2$$

MSE is the Mean Square Error value which is for m × n two multi-tone images I and K in which one of the images is original image and another one is share image. From the above examples, it is clear that the size of both the original image and the recovered image are size

VI. CONCLUSION

The proposed method describes how a secret image is securely communicated from source to destination. The sender has to select the image that should be sent secretly to the receiver. The secret image is splitted into "n" number of shares. Each share is encrypted using XOR operation. Then, all the encrypted shares are transmitted in a single transmission to the receiver. The receiver should use the decryption key to decrypt the shares. After decrypting, the individual shares will be joined together to form the recovered (original) image. The recovered image will be of the same size as the original image.

REFERENCES

1. G. Ateniese, C. Blundo, A. D. Santis and D. R. Stinson (2001) "Extended capabilities for visual cryptography," Theoretical Computer Science, vol. 250, no. 1–2, pp. 143– 161.
2. Beimel and I. Orlov (2011) "Secret sharing and non-shannon information inequalities," IEEE Transactions on Information Theory, vol. 57, no. 9, pp. 5634–5649.
3. M. Bose and R. Mukerjee (2010) "Optimal (k, n) visual cryptographic schemes for general k," Designs, Codes and Cryptography, vol. 55, no. 1, pp. 19–35.
4. O. Farras, T. Hansen, T. Kaced and C. Padro (2014) "Optimal non-perfect uniform secret sharing schemes," in Proceedings of Advances in Cryptology – Crypto 2014, ser. Lecture Notes in Computer Science, vol. 8617. Springer-Verlag, pp. 217–234.
5. M. Sasaki and Y. Watanabe (2014) "Formulation of visual secret sharing schemes encrypting multiple images," in Proceedings of the 39th IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2014). IEEE, pp. 7391–7395.\
6. S. Washio and Y. Watanabe (2014) "Security of audio secret sharing scheme encrypting audio secrets with bounded shares," in Proceedings of the 39th IEEE International Conference on Acoustics, Speech & Signal Processing (ICASSP 2014). IEEE, pp. 7396–7400.
7. Kai-Hui Lee & Pei -Ling Chiu (2011) "A high contrast and capacity efficient visual cryptography scheme for the encryption of multiplesecretimages",Optics Communications, June, Volume 284, Issue 12, p. 2730-2741.
8. Y. C. Chen (2017) "Fully incrementing visual cryptography from a succinct non – monotonic structure," IEEE Transactions on Information Forensics and Security, May vol. 12, no. 5, pp. 1082–1091.
9. C.N. Yang and T.H. Chung (2010) "A general multi- secret visual cryptography scheme," Optics Communications, vol. 283, no. 24, pp. 4949–4962.
10. S. J. Shyu (2014) "Threshold visual cryptographic scheme with meaningful shares," IEEE Signal Processing Letters, vol. 21, no. 12, pp. 1521–1525.
11. Chen T-H, Wu C-S (2011) Efficient multi-secret image sharing based on Boolean operations. Signal Process 91.1:90–97.

Ant Based Routing and QoS Effective Data Collection for Mobile Wireless Sensor Network

Mrs.M Senthamarai Selvi'
Associate Professor,
Department of Computer Science and Engineering
St.Anne's College of Engineering and Technology

Mr.R.Rajarajan, Assistant Professor,
Department of Computer Science and Engineering
St.Anne's College of Engineering and Technology

Ms. N.Hemalatha , Ms. M.Vijayalakshmi,
UG Students,
Department of Computer Science and Engineering
St.Anne's College of Engineering and Technology

Abstract: **Mobility management in Mobile Wireless Sensor Networks (MWSNs) is a complex problem that must be taken into account. In MWSN, nodes move in and out of the network randomly. Hence, a path formed between two distant nodes is highly susceptible to changes due to unpredictable node movement. Also, due to the limited resources in WSN, the paths used for data transmission must be tested for the link quality and time consumed for data forwarding. In order to solve these issues, in this paper, an Ant based routing protocol with QoS effective data collection mechanism is proposed. In this protocol, the link quality and link delay are estimated for each pair of nodes. Link quality is estimated in terms of Packet Reception Rate (PRR), Received Signal Strength Indicator (RSSI) and Link Quality Index (LQI). A reliable path is chosen from the source to the destination based on the paths traversed by forward ants and backward ants. Then, if the link is found to be defective during data transmission, a link reinforcement technique is used to deliver the data packet at the destination successfully. The mobile robots collect the information with high data utility. In addition each mobile robot is equipped with multiple antennas and Space Division Multiple Access (SDMA) technique is then applied for effective data collection from multiple mobile robots. Simulation results show that the proposed routing protocol provides reliability by reducing the packet drop and end-to-end delay when compared to existing protocols.**

I. INTRODUCTION

A Wireless Sensor Network (WSN) consists of several minute sensor nodes which perform functions like monitoring the network surrounding, handling the sensed information, communicating with the destination node wirelessly, etc. The sensor nodes in WSN have limited resources and are basically microelectronic devices. After the deployment of the sensors in WSN, these sensors work independently using batteries with limited energy. Hence, operations such as routing, duty cycle scheduling and medium access controlling must be performed efficiently in WSN [5,10]. WSN can be used in home, military, science, transportation, health care, disaster relief, warfare, security, industrial and building automation, space discovery, etc. WSN is vastly used in phenomena monitoring [8].

Recently, mobile wireless sensor networks (MWSNs) are emerging as a new trend of WSN. They posses all the properties of static WSNs along with node mobility [15]. A major problem in mobile wireless sensor networks (i.e. designed for data-gathering rather than for peer-to-peer sharing) is assessing the 'best' path that a message should take for eventual delivery to a base-station or exit point from the network. Thus delivery is undertaken in a store and forward manner, with nodes exchanging packets on contact with one another. If the mobility patterns of nodes are highly dynamic and essentially unpredictable, determining the optimal path is impossible [3].

Node mobility brings several challenges to large-scale sensor networking.

- The preconstruction of message delivery network may not be useful since the topology may change too frequently due to node movement.
- The frequent location updates from a mobile node can lead to an excessive drain of limited battery power of sensors and increased collisions in wireless transmissions.
- The situation can get worse when the number of mobile nodes grows.
- **Self Configuration:** Once deployed in an unknown area, mobile sensor nodes should configure to cover the area.
- **Agility:** As the phenomena of interest expand, shrink, or migrate to other places, MSN should adjust to the change of the dynamic sensing environment to maximize the sensing coverage.
- **Network Connectivity:** MSNs should have access to a base station to report the current sensing readings. If only a subset of nodes have direct connectivity to the base station, the rest of nodes should have multi-hop paths to those that have that capability.
- **Energy Efficiency:** Energy efficiency is critical to lengthen the network lifetime. Therefore, the traveling distance of mobile nodes and the communication overhead should be minimized.
- **Noise Tolerance:** The sensing environment is subject to a high level of spatial and temporal noise as well as the sensor reading error. Regardless, the MSN should be able to find the optimal location of deployment [12].

II. LITERATURE REVIEW

Getsy S Sara et al [1] have developed a hybrid multipath routing algorithm with an efficient clustering mechanism. A node with higher amount of energy, good communication range and minimum mobility is chosen as the cluster head. The energy consumption during routing is handled efficiently by including the Energy Aware (EA) selection scheme and the Maximal Nodal Surplus Energy determination scheme in this paper. This proposed technique includes the clustering and routing protocol which performs well in highly dynamic environment and also in energy lacking network conditions.

Karim and Nasser [2] have presented a location-aware and fault tolerant clustering protocol for mobile WSN (LFCP-MWSN). At the time of cluster formation and movement of nodes between two clusters, the nodes are localized by the LFCP-MWSN technique by adding a range free mechanism. The energy consumed by this protocol is around 30% lesser when compared with the conventional protocols. The end to end transmission delay involved with this protocol is also low.

Samer Awwad et al [3] have proposed a technique in which the cluster head accepts the data packet from all the nodes in the network during the time slot assigned by TDMA

.

A. Ant Colony Optimization

Ant Colony Optimization (ACO) is a class of algorithms whose first member is called Ant System. When the insects like ants, bees etc., acting as a community, even with very limited individual capability can cooperatively perform many complex tasks necessary for their survival. This new heuristic is robust and versatile in handling a wide range of combinatorial optimization problems [84].

Ant algorithms duplicate the behavior of real ant with a certain number of virtual ants constructing solutions on a construction graph. Each edge in the construction graph is assigned an initial amount of pheromone in the pheromone matrix. After the construction, each solution is evaluated. The better the solution the more pheromone and the corresponding ant may deposit on the edges it traversed during the construction of the solution. This proves that the ants choose these edges in the next iteration of the algorithm.

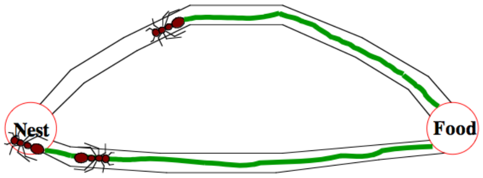


Figure-1 Foraging Behavior of Ants

Once all ants have computed their tour, Ant System updates the pheromone trail using all the solutions produced by the ant colony. Each edge belonging to one of the computed solutions is modified by an amount of pheromone proportional to its solution value. At the end of this phase, the pheromone of the entire system evaporates and the process of construction and update is iterated.

The functions of an ACO algorithm can be summarized as follows:

- ➢ A set of computational concurrent and asynchronous agents (a colony of ants) moves through states of the problem corresponding to partial solutions of the problem to solve.
- ➢ They move by applying a stochastic local decision policy based on two parameters, called trails and attractiveness.
- ➢ By moving, each ant incrementally constructs a solution to the problem.
- ➢ When an ant completes a solution, or during the construction phase, the ant evaluates the solution and modifies the trail value on the components used in its solution.
- ➢ This pheromone information will direct the search of the future ants.

B. Proposed Contributions

In this paper, we propose to design Ant based mobility aided routing protocol for WSN. In this protocol, the link quality is estimated in terms of Packet Reception Rate (PRR), Received Signal Strength Indicator (RSSI) and Link Quality Index (LQI) [7]. In addition to the link quality, the link delay can also be added in the link reinforcement process [6]. In this protocol, for route establishment, the Ant based routing of ant colony optimization (ACO) is used. Here the forward ants (FANT) and back ward ants (BANT) can be used for route request and route reply process, respectively. Figure 2 shows the block diagram of the proposed routing protocol.

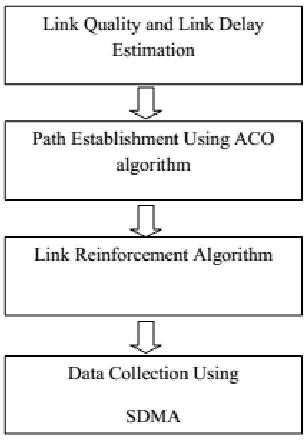

Link Quality and Link Delay Estimation
Path Establishment Using ACO algorithm
Link Reinforcement Algorithm
Data Collection Using SDMA

Figure 2: Block Diagram

C. Link Quality and Link Delay Estimation

The link quality is estimated in terms of Packet Reception Rate (PRR), Received Signal Strength Indicator (RSSI) and Link Quality Index (LQI) [7]. The LQI is estimated according to the equation (1) given below:

$$LQI = PRR \ \times normalized(RSSI_{mean}) \quad (1)$$

where $normalized(RSSI_{mean})$ = $\frac{RSSI_{mean}}{60} + \frac{100}{60}$ (2)

$$RSSI_{mean} \ \in [-100, -40]dbm$$

$$normalized(RSSI_{mean}) \in [0,1]$$

$$PRR \in [0,1]$$

The link delay, D_{link} is calculated according to equation (3) given below:

$$D_{link} = D_{proc} + \ D_{prop} \qquad (3)$$

where D_{proc} is the processing delay involved with the forward ant/ backward ant

D_{prop} is the propagation delay between two nodes

D. Path Establishment for Mobile Robots using ACO algorithm

The path to transmit the data between the source and the destination is determined using the ACO algorithm. When there is need to transmit data, the ant colony is used to discover all the possible paths towards the destination using forward ants and backward ants. The format of the forward ant and backward ant is described in figure (2) and (3).

The pheromone, φ redistributed by backward node is given according to the equation (4) depicted below: $\varphi = \ \varphi + LQI - D_{link}$ (ms) (4)

Based on the LQI value and time used, the path is selected.

Thus, the path from the source to the destination node is determined based on the ACO algorithm which considers the quality of every link used for data transmission. Also, the selected path ensures lower delay in forwarding packets.

E. Link Quality Reinforcement algorithm

Link Quality reinforcement is performed to reinforce the link defects. This is necessary even though the path is determined efficiently using ACO due to the error prone nature of the wireless sensor network. Due to the dynamic network topology, there are possibilities of link compromise. So, link quality reinforcement is used.

Every node maintains a routing table. In the node's routing table, information about its neighboring nodes and surrounding robotic nodes are recorded. The path from the source to destination is selected based on the ACO algorithm and the LQI at every route is estimated. In case of lower LQI, the link quality reinforcement algorithm is used. ***Estimating Data Utility (D_u)***

When a mobile robot enters a sensing field, it performs the function of collecting the data. But, for improved network operation, the data collected need to be of good quality, which is possible only if the data present at each node is of good quality.

Data Utility [16] is a metric estimating the sum of qualities of information from the sensed data divided by communication overhead occurring the network in during data collection. Moreover, it maximizes gathered information without any increase in energy consumption.

F. Data Collection using Space Division Multiple Access (SDMA)

Algorithm:

Notations:

1. P	:	set of subsets of polling points
2. P_i'	:	subset of polling points
3. S_i'	:	sensor nodes
4. i	:	integer value

1. The polling points in the network are selected and grouped according to its current region, into a set of subsets of P denoted by P_1', P_2',….., P_n', such that
$$P_1' \cap P_2' \cap \dots\dots \cap P_n' = \emptyset$$
$$P_1' \cup P_2' \cup \dots\dots \cup P_n' = P' \epsilon P_i$$
2. The sensor nodes in the network are grouped according to its current location and represented by S_1', S_2',….., S_n', such that
$$S_1' \cap S_2' \cap \dots\dots \cap S_n' = \emptyset$$
$$S_1' \cup S_2' \cup \dots\dots \cup S_n' = S' \epsilon S_i$$
3. The mobile robots visit the polling points in the sequence P_i' where i=1, 2 ….., n, such that maximum data gathering time among n regions is minimized.
4. Thus, the overall latency involved in data collection from the sensor nodes is minimized.
5. Then the compatible pair among sensors are determined by connecting two sensors which lie within the coverage area of a single selected polling point.
6. The polling point ensures that the compatible pair of sensors are in a short moving tour.
7. If the sensor pair does not lie within the short moving tour path, then this pair is ignored.
8. This guarantees the latency involved in data uploading to be maintained at a minimum level.
9. By connecting all the polling points, a minimum spanning tree is created and values are allocated to each point of the tree.
10. Then the spanning tree is divided into smaller trees, since the network range is usually too large to be considered a single tree.
11. After the tree size is optimized, the mobile robots traverse through the tree.
12. The mobile robots hop from one polling point to the next polling point, along the tree path.
13. At each polling point, the mobile robot collects data from every compatible sensor pair within the coverage area of the polling point.
14. After gathering data from one polling point, the mobile robot hops to the next polling point and so on.

III. SIMULATION RESULTS

A. Simulation Parameters

We use NS-2 [16] to simulate our proposed Ant based Routing and QoS Effective Data Collection (ARQEDE) protocol. We use the IEEE 802.11 for Mobile Sensor Networks as the MAC layer protocol. It has the functionality to notify the network layer about link breakage. The sensor nodes are randomly deployed over an area of size 500 meter x 500 meter. In the simulated topology, there are 5 mobile robotic nodes and 95 mobile sensors with one static sink or base station, located at the top right corner. The mobile sensors are moving at an average speed of 2m/s and the mobile robots are moving at the speed of 5m/s.

B. Results & Analysis

In this section, the performance evaluation of AMAR and RoCoMAR protocols are presented by varying the data sending rate and number of traffic flows.

1. Varying Data Sending Rate

The data sending rate of CBR traffic is varied from 50 to 250Kb for 10 traffic flows and the performance is evaluated.

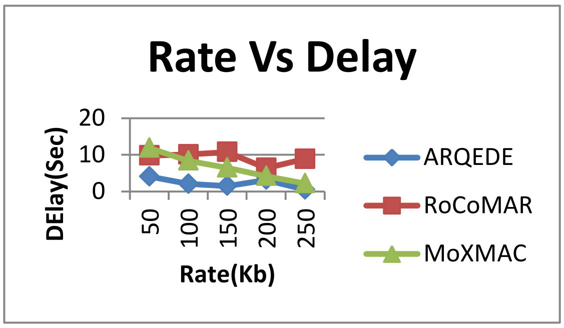


Fig 4: Rate Vs Delay

Figure 4 shows the resutls of delay for ARQEDE,MoXMAC and RoCoMAR protocols, when the rate is varied. Since ARQEDE includes the link delay metric also in path establishment, the associated delay of ARQEDE is 73% lesser when compared to RoCoMAR and ARQEDE is 64% leser when compared to MoXMAC.

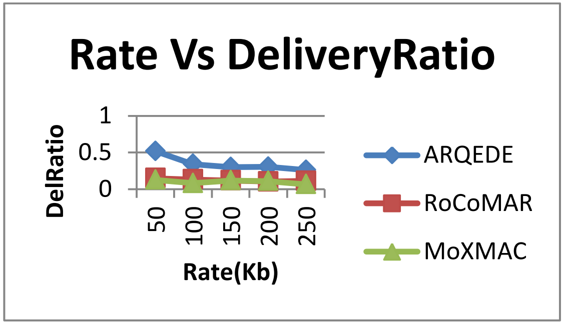


Fig 5: Rate Vs Delivery Ratio

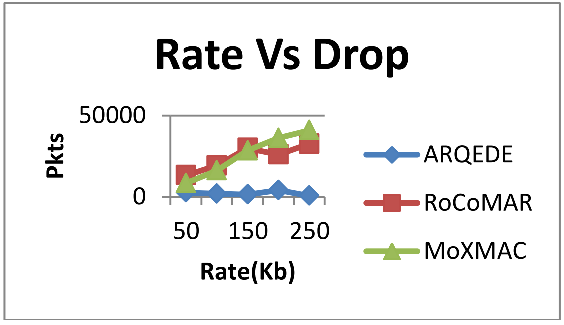


Fig 6: Rate Vs Drop

Figure 5 and 6 show the resutls of packet delivery ratio and packet drop for ARQEDE ,MoXMAC and RoCoMAR protocols, when the rate is varied. As the volume of data traffic increases, there will be more packet drops. As depicted in figure 5 and 6, the packet drop linearly increases for RoCoMAR at higher data rates whereas ARQEDE shows a steady packet drop and delivery ratio. Accurate estimation of link quality in ARQEDE yields 63% higher delivery ratio and 90% lesser packet drops, when compared to RoCoMAR and ARQEDE is 70% is higher delivery ratio than MoXMAC and ARQEDE is 88% lesser packet drops.

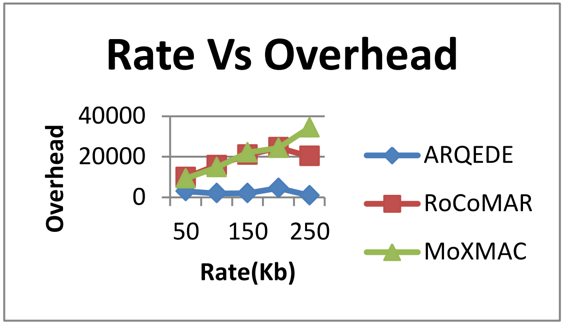


Fig 7: Rate Vs Overhead

Figure 7 shows the results of overhead occurred for ARQEDE,MoXMAC and RoCoMAR protocols, when the data sending rate is varied. The use of ACO technique in ARQEDE reduces the huge packet exchange involved in route discovery. Hence the overhead of ARQEDE is 84% less, when compared to RoCoMAR and 85% less,when compared to MoXMAC.

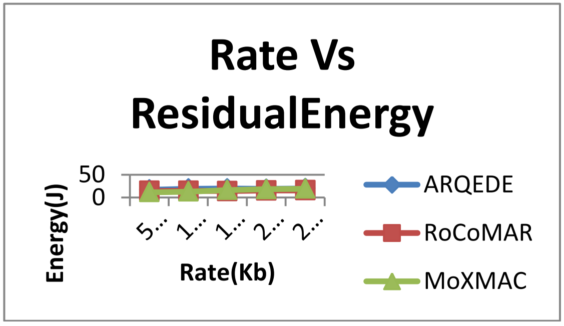


Fig 8: Rate Vs Residual Energy

Figure 8 show the results of residual energy for ARQEDE and RoCoMAR protocols, when the rate is varied. When comparing the performance of the two protocols, we infer that ARQEDE has 21% higher residual energy, than RoCoMAR, since the number of route disconnections is minimized in ARQEDE there by reducing the energy involved in retransmission and 18% higher residual energy then MoXMAC.

2. *Varying the Data Flows*

The number of sources sending data to the sink are varied from 2 to 10 with a data sending rate of 50Kb and the performance is evaluated.

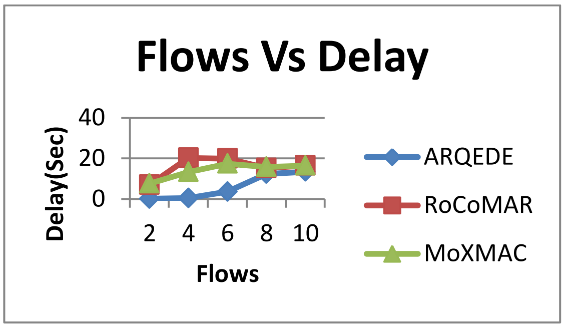


Fig 9: Flows Vs Delay

Figure 4 shows the resutls of delay for ARQEDE,MoXMAC and RoCoMAR protocols, when the rate is varied. Since ARQEDE includes the link delay metric also in path establishment, the associated delay of ARQEDE is 63% lesser when compared to RoCoMAR and ARQEDE is 64% leser when compared to MoXMAC.

IV. CONCLUSION

In this paper, we have proposed ant based mobility aided routing in the wireless sensor network. Initially, the ant colony optimization technique is used to determine a reliable path. The forward ants and the backward ants use pheromone to avoid revisiting any node which may prolong the path. The link quality and delay involved are the important factors used for path selection by the ant colony. After the selection of a path, data packets are transmitted by the source towards the destination node. During data transmission, the link quality is again tested and compared with respect to a predefined value. If the link quality is determined to be poor then robotic nodes are placed in the poor link in between the two consecutive intermediate nodes. This enhances the link quality and makes the link reliable. The data is then delivered at the destination by inserting robotic nodes whenever any link quality is determined to be poor. For QoS effective data collection, each mobile robot is equipped with multiple antennas to apply SDMA technique to collect data with high utility. Simulation results show that the proposed routing protocol provides reliability by reducing the packet drop and end-to-end delay when compared to existing protocols.

REFERENCES

1. Getsy Sara, Kalaiarasi, Neelavathy Pari and Sridharan, "Energy Efficient Clustering And Routing in Mobile Wireless Sensor Network," International Journal of Wireless & Mobile Networks, Vol.2, No.4, 2010
2. L. Karim and N. Nasser, "Reliable location-aware routing protocol for mobile wireless sensor network," The Institution of Engineering and Technology, 2012
3. Samer A. B. Awwad, Chee K. Ng, Nor K. Noordin, and Mohd. Fadlee A. Rasid, "Cluster Based Routing Protocol for Mobile Nodes in Wireless Sensor Network," IEEE, 2009
4. Peng Li and Xu Jian-bo, "ECDGA: An energy-efficient cluster-based data gathering algorithm for Mobile Wireless Sensor Networks," IEEE International Conference of Computational Intelligence and Software Engineering, 2009.
5. Papa Dame Ba, Ibrahima Niang and Bamba Gueye, "An optimized and power savings protocol for mobility energy-aware in wireless sensor networks," Springer, Telecommunication System, 2013

6. Duc Van Le, Hoon Oh and Seokhoon Yoon, "RoCoMAR: Robots’ Controllable Mobility Aided Routing and Relay Architecture for Mobile Sensor Networks," Sensors, 2013
7. Michele Rondinone, Junaid Ansari, Janne Riihij arvi and Petri Mahonen, "Designing a Reliable and Stable Link Quality Metric for Wireless Sensor Networks, "Proceedings of the workshop on Real-world wireless sensor networks, ACM, 2008
8. Xing Zhang, Jingsha He and Qian Wei, "Energy-Efficient Routing for Mobility Scenarios in Wireless Sensor Networks," In Proceedings of the Third International Symposium on Electronic Commerce and Security Workshops, 2010

Smart Classrooms Access Control over Near Field Communication in IOT

Ms. T.Hemalatha, Mr. V.Gopikrishnan, Mr. N.Thanigaivel
Assistant Professor,
Department of Computer Science and Engineering,
Krishnasamy College of Engineering and Technology.

Abstract: The Internet of Things is one of the ideas that has become increasingly relevant in recent years. It involves connecting things to the Internet in order to retrieve information from them at any time and from anywhere. In the Internet of Things, sensor networks that exchange information wirelessly via Wi-Fi, Bluetooth, Zigbee or RF are common. In this sense, our paper presents a way in which each classroom control is accessed through Near Field Communication (NFC) and the information is shared via radio frequency. These data are published on the Web and could easily be used for building applications from the data collected. As a result, our application collects information from the classroom to create a control classroom tool that displays access to and the status of all the classrooms graphically and also connects this data with social networks.

Keywords: Internet of Things; NFC; Arduino; sensors; smart environment; classroom access control

I. INTRODUCTION

The effective management of classrooms, halls, offices, and public spaces in any institution or building is often a difficult problem. There are many rooms of different types within a building; therefore, recording the activities undertaken in them in real-time is usually intricate. Thus the smart room concept described in this paper tries to solve this problem by using sensing solutions, intelligent environments or decision making environments [1,2]. Furthermore, there are many classrooms or labs in universities with a variety of equipment and purposes that are used for several subjects during an academic year. Though these classes are assigned at the beginning of the year, this can usually be changed throughout the course. When any change occurs, it is difficult to communicate within the institution and the wider university community.

As already stated, the main objective of this work is to provide each classroom with a system to collect information about its real time use: establish a user identification method in each room that can be accessed from the centre, using items that the university already has, take advantage of the opportunities that the Internet of Things provides by creating an application to record the use of the classrooms. This article is organized as follows: in Section 2 the technologies involved are introduced. In Section 3 the proposed architecture for classroom access control is specified. Section 4 concludes with the work completed as well as the proposals for future work.

1.1. Technologies at Work

In this section each of the technological aspects mentioned in this paper (the Internet of Things, Arduino, Web 2.0 and NFC) is analyzed in turn.

The Internet of Things

In the beginning, the Internet was only designed for communication in which computers could access websites, download content or communicate with other users. However, technologies evolve creating more powerful devices, faster and with more capabilities. Advances in electronics technology

are also creating smaller devices with low power consumption which means that large networks of sensors can be created, with the ability to obtain information, process it and act accordingly. Here it is how the idea of the Internet of Things arises [3]. This term was coined in 1999 by Kevin Ashton, cofounder of Auto-ID Center at the Massachusetts Institute of Technology (MIT) [7] bearing in mind the concept of ―ubiquitous computing‖ [8,9]. Under this term, computers and technologies are around users without noticing their presence, being able to cooperate and adapt their behaviors to the environment and enabling users to interact with technology without interfering with their everyday life. In this sense, the concept of computer as hardware device is diluted to integrate connected devices around and in cooperation with users' daily life.

Arduino

The open hardware platform Arduino is closely related to the previous section [12]. Arduino is a platform that seeks simplicity when creating applications by using a combination of software and

hardware; it is based on a board with a single microcontroller input/output pin for communication and control of physical objects and the environment. This kind of device has been developed to connect all kinds of objects and its functionality directly relates it to the Internet of Things.

Web 2.0 and Mashups

The term Web 2.0, attributed to Tim O'Reilly [15], arises from the concept that the Web should be an ―architecture of participation‖, a platform for information that allows innovation by independent developers. The idea was also that it was free of use, to allow more people to participate, combined with the concept of mobility as many users from different places can be involved.

Web 2.0 refers to those websites that facilitate information sharing, interoperability, user-centered design and collaboration with the World Wide Web. This term includes communities, services and Web applications, social networking, video hosting services, wikis, blogs, mashups and folksonomie. Some of these associated services include:

- Blogs: they are personal spaces where authors can write articles and news in chronological order and a collaborative space where readers participate.
- Wikis: a collective website construction with a specific topic, in which users are free to add, remove or edit content.
- Social Networking: Web sites where each user has their own page which allows them to post content and communicate with other users.
- Resource sharing environments: they are places to store all kinds of data in order to share and

  view them from anywhere (documents, videos, photos, *etc.*).
- Folksonomies: is the work of tagging Web content. The value of this action lies in that people can use their own vocabulary to explicitly add value to the content they are consuming.

In Web 2.0 there are two technologies widely used to exchange data between applications, JSON or XML:

- XML (eXtensible Markup Language) is a software technology based on information derived from SGML language and developed by the World Wide Web Consortium. The files are XML documents whose information is organized in a tree which is used for exchanging structured information on different platforms and could be validated with XML-Schemas. In fact XML is a meta-language that could be used to define our own communication language.
- JSON, JavaScript Object Notation, is a lightweight alternative to XML format for sending or
receiving data. JSON belongs to a subset of the object literal notation of JavaScript. JSON is a collection consisting of pairs of name/value. Since these structures are in any programming language, we can say that the exchange of data using JSON is independent of the programming language used. This has been one of the keys to its growing popularity if simplicity is sought.

Near Field Communication

Near field communication (NFC) is a wireless short-range and high frequency communication technology that allows the exchange of data between devices. This technology is based on electromagnetic fields [5] that usually communicate by using an identification card with a reader. The standard governing the use of electronic identification cards and smart cards is ISO 14443 (RFID), which is managed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and FeliCa. NFC works in the field of 13.56 MHz and shares the characteristics of the ISO 14443.

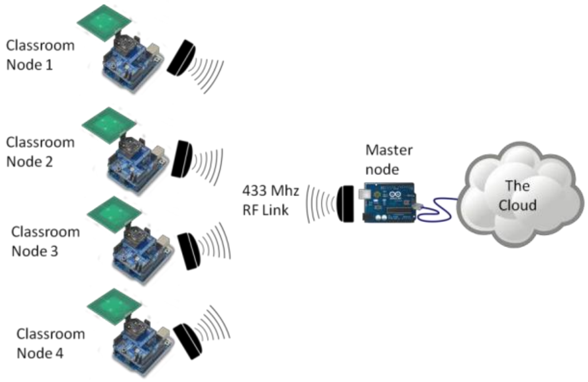
The maximum range of NFC is 20 cm. Although this may seem to be a disadvantage, it does not have to be, as this is what leads to improved security. Also NFC teams are able to send and receive information simultaneously. Because NFC devices must be in close proximity to each other, usually not more than a few centimeters, they have become a popular choice for secure communication between consumer devices such as Smartphones. In our case, MiFare cards are selected since are extensively used in access control for office buildings, payment systems for public transport, as well as other applications [18].

II. ARCHITECTURE DESIGN FOR CLASSROOMS ACCESS CONTROL

The operation of this project is governed by the functionality of the Internet of Things [3]. Our classrooms registration system is based on a network of connected sensors that collect information that is then uploaded to the cloud so that any application can use this information when necessary. This scheme has two distinct parts which include:

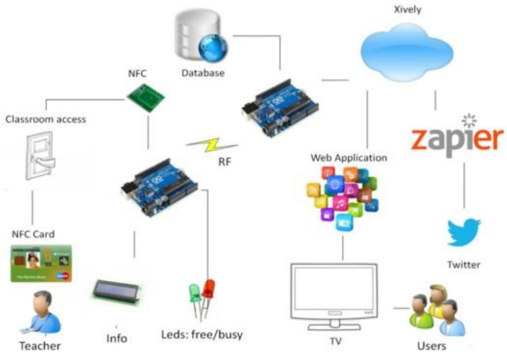
- The ―thing‖, which contains in our case is the classroom and its access.
- The cloud, which are Internet applications where the data is stored.

Figure 2. System communication scheme.



In more detail, the system would start working when trying to access a classroom (Figure 3), a process where an ID card would be used for this purpose. The user uses an NFC card reader connected to the Arduino device that shows a message on the LCD screen and one of the LEDs lights up, showing that the classroom is in use (red LED).

Figure 3. Overall system.



Immediately afterwards, the Arduino device connects to another Arduino (Master) by radio to identify the user accessing the classroom system. The system will use this ID to connect to the database and check whether it is a teacher and retrieve their name.The next step is sending the data to the cloud, transferring the name of the teacher and the classroom to the server platform Xively [19] to be conveniently stored.

From the data stored in Xively, two applications are created. On the one hand, Google Maps is used for retrieving data from Xively to create a map of the university showing the classroom information. This application can be accessed from any computer and the contents can be displayed on the university information screens (TV panels).On the other hand, an application could send messages with information from each classroom by taking advantage of the social network Twitter (tweets). To help us accomplish this task, the tool Zapier is used [20].

Hardware

In this section the hardware used in the two types of nodes is described. Classroom nodes that read the card sent by RF are composed of (Figure 4):

- Arduino UNO.
- NFC module for Arduino and communication shield from cooking-hacks [21].
- LCD screen,
- Two LEDs (Red and Green),
- Radio Frequency module (433 MHZ).

Reading Data (NFC)

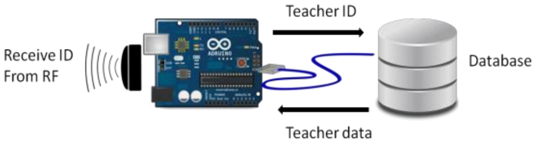
The collection of data through user interaction with an NFC reader is the initial offstage in the system. The description of the reader and how it works is presented below. Our NFC reader consists of an Arduino Uno, a Xbee shield with an NFC reader, a radio frequency module, an LCD display and two LEDs. Before attempting to access the classroom, it could be either free or occupied. If it is free it will be possible to complete the identification process and access the classroom.

. ***Processing Data***

The master node is the destination of the data that the NFC reader has obtained and sent by radio frequency. The master consists of an Arduino Ethernet and RF module with a receiving antenna (Figure 7).

Initially, the receiver will connect to the network by using its Ethernet connection and prepare the necessary pin (pin 2) for receiving data via radio frequency. Once done, it will remain in standby until it receives the data.

Once the receiver has collected data by the NFC reader, it must perform processing to complete this information. Keep in mind that when reading NFC, it is transmitting the identification code for each user and the classroom they want to access, while finding the name of the user involves consulting the database hosted on the server. To place a PHP service in the same server through an HTTP request from our Arduino, the user name and related information will be returned when the ID is received from the reader. This information will be required to store data in the cloud, as discussed in the following section. In order to get a good performance in the master node, the data is uploaded to the cloud immediately and no information is saved on it (Figure 6(b)).



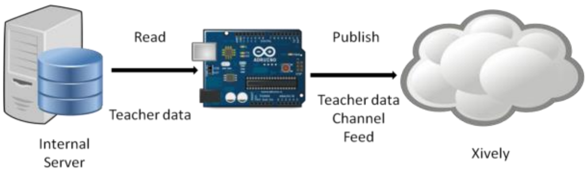
Data in the Cloud

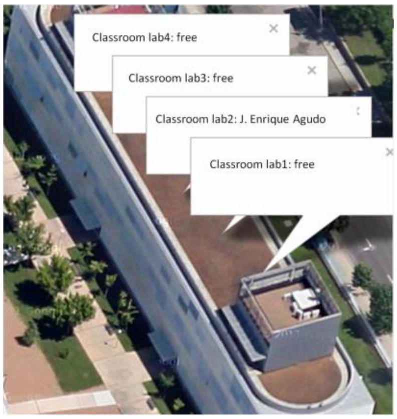
Since the major goal of this project is mainly focused on the access to the classroom by teachers, the response from the server database to the http request can only contain the teacher's name. Thus,   if the person were not registered in the database, it would imply that such user is not a teacher, or an authorized person, and access would not be consequently registered.

The explanation of how the Xively server works is briefly described below. Xively provides a working environment in which you can create a new project for each application. Each project consists of a number of variables called –channels‖ that store the values of our applications. In our case, a channel for each classroom that we will use is created.

The program created in Arduino, takes the name of the teacher as a variable and uses the PUT function of Xively and the appropriate parameters (key to our account on the server and classroom ID) to update the server data (Figure 8). To make use of these functions, first the Xively page is checked to obtain a password to use their API, then the project is identified as –feed‖ and the Xively library to Arduino is downloaded.

Figure 8. Putting data in the cloud.





• *Using the Data: Google Maps App*

In order to use API Xively, it will be necessary to establish the same values as in the previous section: the project feed and the API key.

III. CONCLUSIONS AND FUTURE WORK

A tool and a device have been developed to manage classrooms in real time. To do this, a transmitter/receiver access control for each classroom has been created, data are uploaded to the cloud and a Web application to view the data has been built.

Arduino hardware has provided enormous simplicity in the development of the prototype. The different modules and shields are successfully integrated. The programming of the device was not complicated as the Arduino developer community is large and there are many tutorials that can be accessed via the net.

The result is that a thing, the classroom, registers information in the cloud via a sensor network created with Arduino components. Different applications that make use of data by integrating them into an application that uses Google Maps to produce information published on Twitter has been developed. This not only shows the possibilities of the Internet of Things but also scalability and reuse of data that can be generated. Also NFC, RF, Arduino, Xively, Google Maps and Zapier technologies are combined in the same project with a successfull result that tests the power of the Internet of Things for managing and sharing data.

In addition, by placing motion sensors, or sensors that measure temperature, sound or light, to detect use, would remove the need for the teacher to swipe a card when entering the classroom. In the application server and Xively, the subject and schedule of teacher could be added, as well as the equipment needed and the student roster.

Finally, the data shared in social networks could be used for additional purposes by combining it with other applications such as updating the school Google Calendar.

REFERENCES

1. Ramos, C.; Marreiros, G.; Santos, R.; Freitas, C.F. Smart Offices and Intelligent Decision Rooms. In Handbook of Ambient Intelligence and Smart Environments; Nakashima, H., Aghajan, H., Augusto, J.C., Eds.; Springer: New York, NY, USA, 2010; pp. 851–880.
2. Reijula, J.; Gröhn, M.; Müller, K.; Reijula, K. Human well -being and flowing work in an intelligent work environment. Intell. Build. Int. 2011, 3, 223–237.
3. Doukas, C. Building Internet of Things with the Arduino; CreateSpace: North Charleston, SC, USA, 2012.

New Models for Human- computer Interaction

Mr. S.Manavalan
Associate Professor,
Department of Computer Science and Engineering,
St. Anne's College of Engineering and Technology

Ms.N.Akila, Ms.E.Amala Sharini
UG Students,
Department of Computer Science and Engineering,
St. Anne's College of Engineering and Technology

Abstract - A person's interaction with the outside world occurs through information being received and sent: input and output. In an interaction with a computer the user receives information that is output by the computer, and responds by providing input to the computer – the user's output becomes the computer's input and vice versa. Human Computer Interaction is a methodology to how the people interact with computer. This paper reviews and classifies the existing models. This paper proposes some new approaches to the models of human computer interaction.

***Index Terms* - HCI- Human-computer interaction.**

I. INTRODUCTION

In the early days of computing, information was entered into the computer in a large mass – batch data entry. There was minimal interaction with the machine: the user would simply dump a pile of punched cards onto a reader, press the start button, and then return a few hours later.

This still continues today although now with pre-prepared electronic files or possibly machine-read forms.

Human-computer interaction is the major challenge in the era of computing. It is concerned with the joint performance of tasks by humans and machines .The human computer interaction can be described as focus the point of communication between the human user and the computer. The information between the human and computer is defined as the loop of interaction. The loop of interaction has several aspects, including Visual Based, Audio Based ,Task environment, Machine environment and Areas of the interface .

According to the following statements illustrate the base of the human computer interaction:

- The Human Computer interaction depend on the users attitudinal responses.
- Using social intelligence device to get positive feedback.
- Telecommunication level interaction is always low.
- Find balance between useful interruptions and attention for co-located persons
- The low level of alert only needed.

This paper focuses on the human computer interaction problem and classifies the existing models. Moreover, we propose some new approaches to the model of human computer interaction. The objectives of this paper are

- To classify the existing model of human computer interaction
- To describe a meta-Sensor based model of human computer interaction
- Propose a six-senses based model of human computer interaction

II. MODELS OFHUMAN COMPUTER INTERACTION

The two main types of HCI are internal HCI and external HCI.Here we see about some types of internal HCI models are Traditional model, Sensor based model, creative model, meta-post Traditional model, and six-senses based model. in the following sections we explain the property of the mentioned models.

2.1 Traditional Model

Traditional model human computer interaction is the traditional method of interactions. In this method interactions have a low level of transparency. This form of interaction is not quiet secure and reliable. A simple form of Traditional model human computer interaction is shown in Fig 1. As the figure shows the human and computer have an explicit form of interaction. The following list indicates some advantages and disadvantages of this kind of human computer interaction:

- Low Cost
- Easy to Implementation
- Low Security
- Low Transparency
- Low Integrity
- Low Complexity of Computation
- High Complexity of Interaction

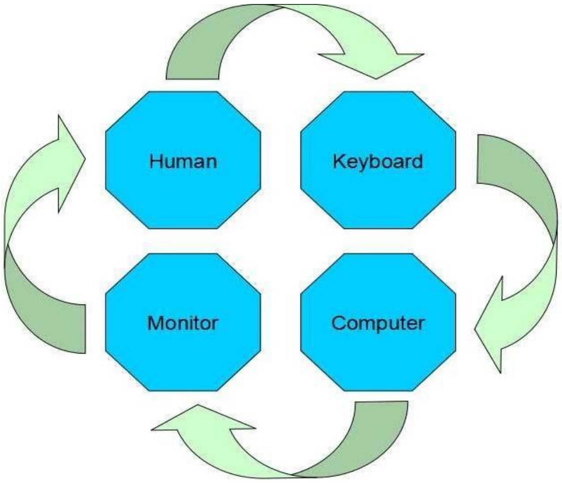


Fig. 1. Traditional base human computer interaction

An example of this kind of human computer interaction has been shown in Fig 2.

Fig. 2. The user puts an ATM-card in the machine. The ATM machine identifies the user only by using the card.

2.2 Sensor based Model

In this form of human computer interaction we use advanced device for communicating. The information can be captured by using a set of sensors. The captured data must be analyzed and compiled to raw data. For this purpose we use intelligent computation methods. There is a short conversation between user and machine. The conversation also must be translated to raw data. The raw data will be processed by soft-wares and hard wares. For this purposes we use the intelligent computation and algorithms. The following list indicates some advantages and disadvantages of this kind of human computer Interaction:

- High Complexity of Computation
- High Security
- High Transparency
- High Integrity
- Low Complexity of Interaction

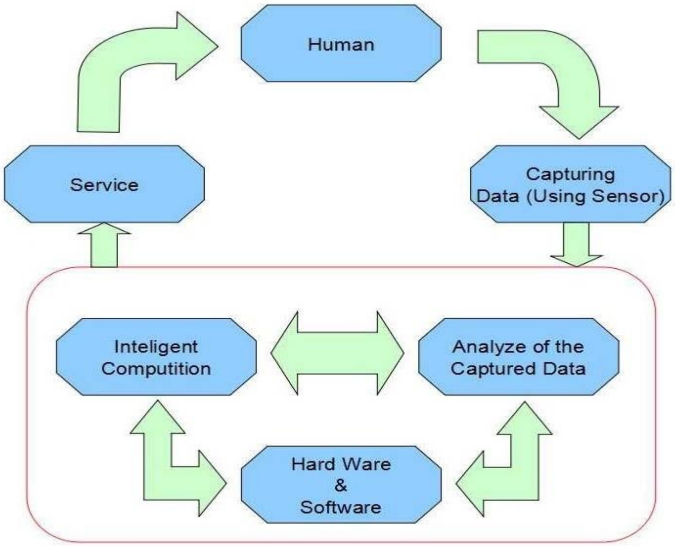


Fig. 3. Sensor based model human computer interaction.

As an example we assume that the user wants to take money from ATM. In this case the user does not need to input a card to the ATM. The ATM captures information related to the user by sensors. There is a short conversion between the user and ATM-machine. The conversion will get translated to the low level information. A simple form of Sensor based human computer interaction is shown in Fig 4.

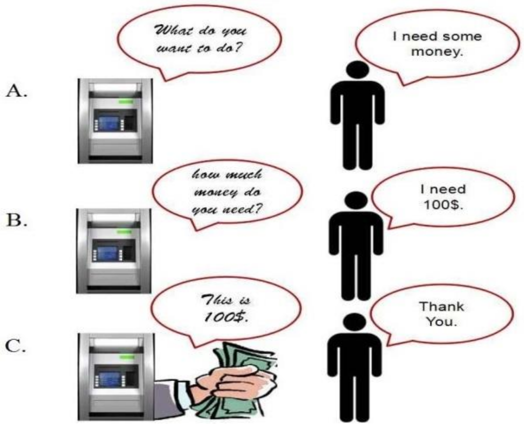


Fig. 4. A simple form of Sensor based human computer interaction.

2.3 Creative Model

Similar to the previous model, in this form of human computer interaction, the machine and user have a conversation too. This conversation usually is very long and complicated. The machine helps to the user to make a decision n order to provide the service that the user needs. For this purpose the cognation based algorithms will be very useful.

Fig 5 indicates a simple example of a creative model of human computer interaction. In this example the person wants to take some money from ATM. We assume that the user does not know how much money he needs. He only tells his plan to machine and the machine will give the enough money to buy what he needs.

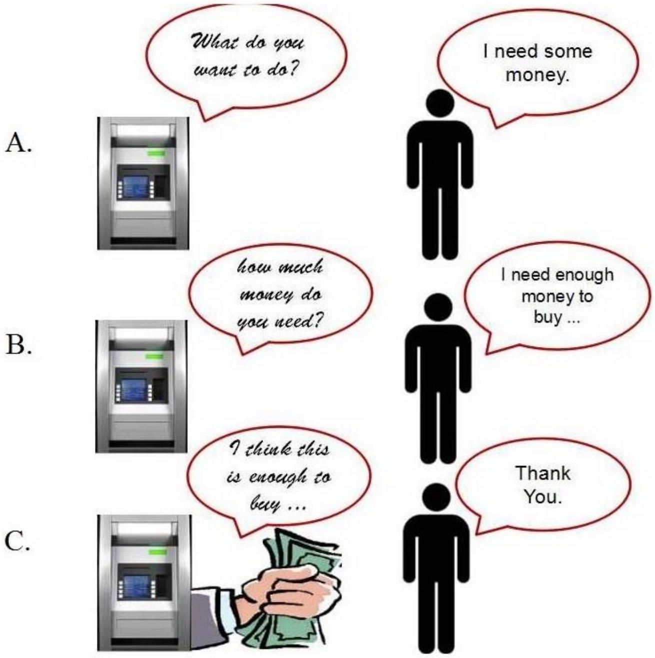

A.
What do you want to do?
I need some money.
B.
how much money do you need?
I need enough money to buy ...
C.
I think this is enough to buy ...
Thank You.

Fig. 5. A simple example of a creative model of human computer interaction.

2.4 Meta-Sensor based Model

In this form of human computer interaction we use advanced sensors for communicating. It can be implemented similar to a brain interface model. The query can be captured from human brain directly. For this purposes a set of intelligent sensors would be used. In this case the interactions have a high level of transparency. The captured information will be analyzed and translated to the raw data. The raw data will be processed by low level soft-wares and hard wares. After that the low level software and hard-wares provide responses. The provided response will be translated to a higher level response. For this purposes a set of middle wares is required. Finally, the high level responses will be considered as a feedback of captured queries. Fig 6 indicates a general model for meta sensor based model human computer interaction.

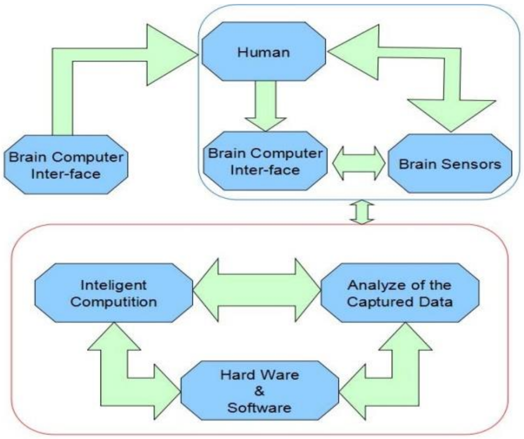

Human
Brain Computer Inter-face
Brain Computer Inter-face
Brain Sensors
Inteligent Computition
Analyze of the Captured Data
Hard Ware & Software

Fig. 6. Meta-Sensor based model human computer interaction.

Fig 7 indicates a simple example of a meta-Sensor based model of human computer interaction. In this case we assume that the user wants to take money from an ATM too. He has to go in Traditional of the ATM. Then the ATM automatically captures the user request and gives money to the user. The person does not do anything. In fact the person does not input any data.

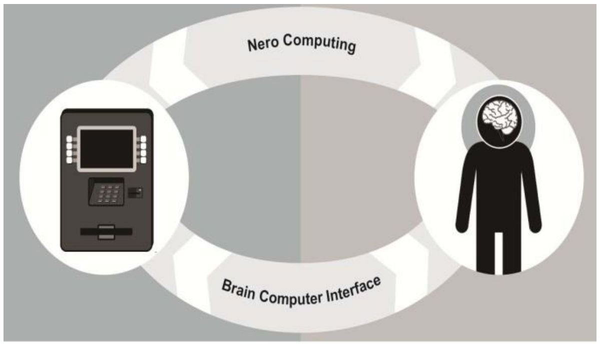


Fig. 7. A simple example of a meta-Sensor based model of human computer interaction.

2.5 Six-senses Based Model

In this form of human computer interaction we assume that that the computers are able to predict natural phenomena. Then by using the predicted information the computers will be able to match the natural phenomena with the human requests. We also assume a brain computer interface model in order to captured the requests of the users. Fig 8 indicates a general model for six-senses based model human computer interaction. The following list indicates some advantages and disadvantages of the six-senses based model human computer interaction

- High Cost
- Difficulty of Implementation
- Risk-able Security
- Very High Transparency
- Complexity of Computation
- Legality Problems
- Very Flexible

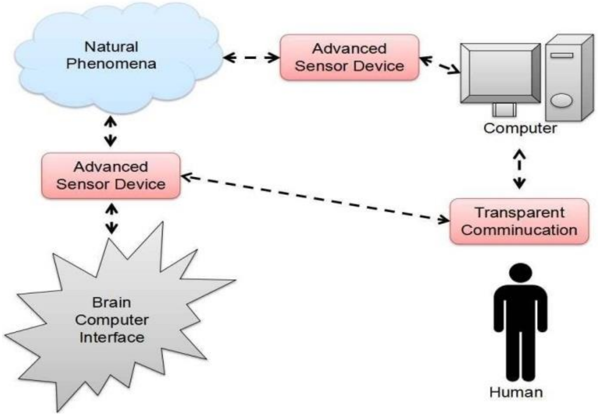


Fig. 8. The model of 6th sense based human computer interaction

III. CONCLUSION

The human computer interaction can be described as the point of communication between the human user and the computer. This paper classified the human computer interaction into five main categories. The paper also provided a general model for each mentioned type of human computer interaction. We also proposed some new model for the implicit human computer interaction.

REFERENCES

1. Dennebouy, Yves, Martin Andersson, Annamaria Auddino, Yann Dupont, Edi Fontana, Massimo Gentile, and Stefano Spaccapietra. "SUPER: Visual interfaces for object+ relationship data models." Journal of Visual Languages & Computing 6, no. 1 (1995): 73-99.
2. Börner, Katy, and Chaomei Chen. "Visual interfaces to digital libraries." In Proceedings of the 2nd ACM/IEEE-CS joint conference on Digital libraries, pp. 425-425. ACM, 2002.
3. Chittaro, Luca. "Interacting with Visual Interfaces on Mobile Devices." Human-Computer Interaction Symposium. Springer US, 2008.Chittaro, Luca. "Interacting with Visual Interfaces on Mobile Devices." In Human-Computer Interaction Symposium, pp. 1-5. Springer Boston, 2008.
4. Clavel, Chloé, Thibaut Ehrette, and Gaël Richard. "Events detection for an audio-based surveillance system." In Multimedia and Expo, 2005. ICME 2005. IEEE International Conference on, pp. 1306-1309. IEEE, 2005.
5. Dix, Alan. "Human-like computing and human---computer interaction." In Proceedings of the 30th International BCS Human Computer Interaction Conference: Fusion!, p. 52. BCS

Learning & Development Ltd., 2016.

6. Bourgeois, L. Jay. "Strategy and environment: A conceptual integration." Academy of management review 5, no. 1 (1980): 25-39.
7. Menon, Aravind, Jose Renato Santos, Yoshio Turner, G. John Janakiraman, and Willy Zwaenepoel. "Diagnosing performance overheads in the xen virtual machine environment." In Proceedings of the 1st ACM/USENIX international conference on Virtual execution environments, pp. 13-23. ACM, 2005.
8. Young, Jason E., G. Arturo Sánchez-Azofeifa, Susan J. Hannon, and Ross Chapman. "Trends in land cover change and isolation of protected areas at the interface of the southern boreal mixedwood and aspen parkland in Alberta, Canada." Forest Ecology and Management 230, no. 1 (2006): 151-161

KNN Classification over Semantic Encryption of Data

Mrs.D. Pauline Freeda
Associate Professor,
Department of Computer Science and Engineering
St. Anne's College of Engineering,Panruti.

Mr.X.MartinLourduraj
Assistant Professor,
Department of Computer Science and Engineering
St. Anne's College of Engineering,Panruti.

Mr.S.Vinothraj, L.Murugan
UG Students,
Department of Computer Science and Engineering
St. Anne's College of Engineering,Panruti.

Abstract - Data Mining is used for extracting potentially useful information from raw data. The integration of data mining techniques into normal day-to-day activities has become common place. Every day people are confronted with targeted advertising, and data mining techniques help businesses to become more efficient by reducing costs. Cloud computing provides a powerful, scalable and flexible infrastructure into which one can integrate, previously known, techniques and methods of Data Mining. We focus on solving the classification problem over encrypted data. In particular, we propose a secure k-NN classifier over encrypted data in the cloud. The proposed protocol protects the confidentiality of data, privacy of users input query, and hides the data access patterns. To the best of our knowledge, our work is the first to develop a secure k-NN classifier over encrypted data under the semi-honest model. a novel secure k-nearest neighbor query protocol over encrypted data that protects data confidentiality, users query privacy, and hides data access patterns. However, as mentioned above, PPk-NN is a more complex problem and it cannot be solved directly using the existing secure k-nearest neighbor techniques over encrypted data. We extend our previous work and provide a new solution to the PPkNN classifier problem over encrypted data

Index Terms – **Cloud, Data mining, KNN query process**

I. INTRODUCTION

Due to the rise of various privacy issues, many theoretical and practical solutions to the classification problem have been proposed under different security models.With the recent popularity of cloud computing, users now have the opportunity to outsource their data in encrypted form as well as the data mining tasks to the cloud.

Data mining is a powerful new technique to discover knowledge within the large amount of the data. Also data mining is the process of discovering meaningful new relationship, patterns and trends by passing large amounts of data stored in corpus, using pattern recognition technologies as well as statistical and mathematical techniques. Data mining sometimes called data or knowledge mining. Data are may be numbers, or sequence of characters that can be processed by a computer.

Nowadays cloud computing model is changing the structure of the organizations way of storing, accessing, and processing their data. As the growing processing data, many organizations to focus on the cloud computing in terms of its efficiency, flexibility, security, and document control.To reduce the data overhead the companies offload their data to the cloud. Most often, organization give their computational activity in addition to their data to the cloud. For all massive advantages of cloud computing provide, privacy and security problems in the cloud are blocking organization.

1.1. Cloud Security

With the recent popularity of cloud computing, data owners now have the opportunity to outsource not only their data but also data processing functionalities to the cloud. Because of data security and personal privacy concerns, sensitive data (e.g., medical records) should be encrypted before being outsourced to a cloud, and the cloud should perform query processing tasks on the encrypted data only. These tasks are termed as Privacy-Preserving Query Processing over encrypted data. Based on the concept of Secure Multiparty Computation (SMC), SMC-based distributed protocols were developed to allow the cloud to perform queries directly over encrypted data. These protocols protect the confidentiality of the stored data, user queries, and data access patterns from cloud service providers and other unauthorized users. Several queries were considered in an attempt to create a well-defined scope. These queries included the k-Nearest Neighbor (kNN) query, advanced analytical query and correlated range query.

1.2 Privacy Preserving Data Mining

Privacy-Preserving Data Mining (PPDM) is defined as the process of extracting or deriving knowledge about data without compromising the privacy of the data. In the past decade, a number of PPDM techniques have been proposed to facilitate users in performing data mining tasks in privacy-sensitive environments. Agrawal and Srikant [10] were the first to introduce the notion of privacy-preserving under data mining applications. An existing PPDM techniques can be classified into two broad categories: data perturbation and data distribution

II. EXISTING SYSTEM

2.1. PrivacyPreserving Data Mining

Existing work on privacy-preserving data mining (PPDM) either perturbation or SecureMulti-party Computation (SMC) based approachcannot solve the DMED problem. Perturbed data do not possess semantic security, so data perturbation techniques cannot be used to encrypt highly sensitive data. Also the perturbed data do not produce very accurate data mining results. Secure multi-party computation based approach assumes data are distributed and not encrypted at each participating party.

2.2.Disadvantages

- In the existing methods, data are partitioned (in plaintext format) among different parties, whereas in this work, they are assumed to be encrypted and stored in the cloud.
- They fail to produce accurate data mining results because some amount of information is lost due to the addition of statistical noises (in order to hide the sensitive attributes).

- Data access patterns can be leaked. The cloud can easily derive useful and sensitive information about usersdata items by simply observing the data access patterns.

III. PROPOSED SYSTEM

In general, it is very difficult to process encrypted data without ever having to decrypt it. The question here is how the cloud can execute the queries over encrypted data while the data stored at the cloud are encrypted at all times.The various techniques related to query processing over encrypted data have been proposed, including range queries and other aggregate queries. These techniques, however, are either not applicable or inefficient to solve advanced queries such as the kNN query

We proposed a novel PPk-NN protocol, a secure k-NN classifier over semantically secure encrypted data.The encrypted data are outsourced to the cloud in the proposed protocol.A secure k-nearest neighbor query protocol over encrypted data protects data confidentiality, users query privacy, and hides data access patterns.The goal of the PPk-NN protocol is to classify usersquery records usingD0in a privacy-preserving manner.

Different distance metrics can be used, depending on the nature of the data. Euclidean distance is typical for continuous variables, but other metrics can be used for categorical data. Specialized metrics are often useful for specific problems, such as text classification. When an instance whose class is unknown is presented for evaluation, the algorithm computes its k closest neighbors and the classis assigned by voting among those neighbors. To prevent ties, one typically uses an odd choice of k for binary classification.

For multiple classes, one can use plurality voting or majority voting. The latter can sometimes result in no class being assigned to an instance, while the former can result in classifications being made with very low support from the neighborhood. One can also weight each neighbor by an inverse function of its distance to the instance being classified.

3.1. KNN Classifier

Here, the problem of secure processing of kNN query over encrypted relational data in a cloud was addressed. That is, given a user' s encrypted query record (q), the objective of the secure kNN problem is to securely identify the top k-nearest (closest) records to q using the encrypted database (T0) in the cloud without allowing the cloud to learn anything regarding either the actual contents of the database (T) or q.

3.2. KNN Algorithm

The k-NN algorithm is unusual from a classification perspective in its lack of explicit model training. While a training dataset is required, it is used solely to populate a sample of the search space with instances whose class is known. No actual model or learning is performed during this phase.These algorithms are also known as lazy learning algorithms for this reason.

STEPS: PPkNN(D^1;q)->c_q

```
Require: $C_1$ has $D^1$ and $\pi$; $C_2$ has $sk$; Bob has q
1: Bob:
    a) Compute $E_{pk}(q_j)$, for $1 \le j \le m$
    b) Send $E_{pk}(q)=(E_{pk}(q_1),...,E_{pk}(q_m))$ to $C_1$
2: C1 and C2:
    a) $C_1$ receives $E_{pk}(q)$from Bob
    b) for i = 1 to n do:
    $E_{pk}(d_i) \leftarrow SSED(E_{pk}(q),E_{pk}(ti))$
    $[di] \leftarrow SBD(E_{pk}(d_i))$
```

```
3: for s = 1 to k do:
a) C1 and C2:
        ($[d_{min}]$,$E_{pk}(I)$, $E_{pk}(C_1)$) ← $\mathbf{SMIN}_n(\Theta_1,....,\Theta_n)$,  where
        $\Theta_i$=([ di], $E_{pk}(I_{ti})$, $E_{pk}(t_{i,m})$)
        $E_{pk}(C^1s) \leftarrow E_{pk}(c^1)$
b) C1:
        $\Delta \leftarrow E_{pk}(I)^{N-1}$
                for i =1 to n do:
                ─$t_i \leftarrow E_{pk}(i)* \Delta$
                ─ $t^1_i \leftarrow t^{ri}_i$ , where $r_i €_R$ ZN
                $\beta \leftarrow \pi(t^1)$; send $\beta$ to $C_2$
c)C2:
                $\beta_i \leftarrow D_{sk}(\beta_i)$, for $1 \le i \le n$
                Compute $U^1$, for $1 \le i \le n$:
            ─ if $\beta^i = 0$, then $U^1_i = E_{pk}(1)$
            ─ otherwise, $U^1_i = E_{pk}(0)$
Send $U^1$ to $C_1$
   d). $C_1$: $V \leftarrow \pi^{-1}(U^1)$
   e). C1 and C2, for $1 \le i \le n$ and $1 \le \gamma \le l$:
        $E_{pk}(d_{i,\gamma}) \leftarrow$ SBOR($V_i$,Epk$E_{pk}(d_{i,\gamma})$)
 4: $SCMC_k(E_{pk}(c^1_1),..., E_{pk}(c^1_k))$
```

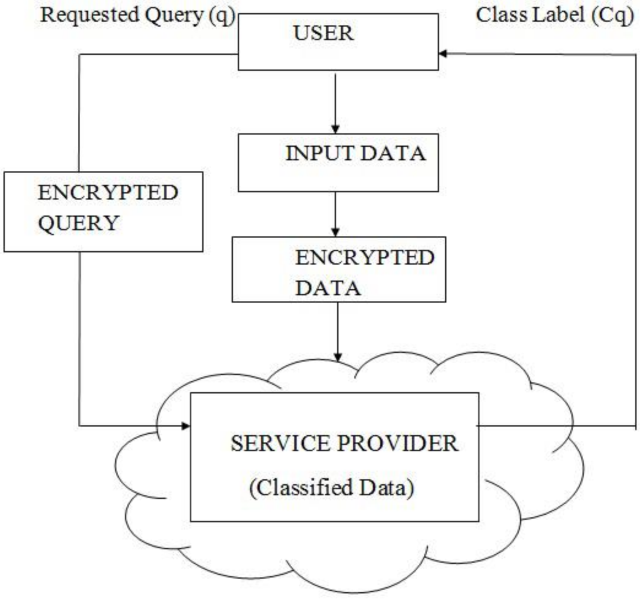


Fig 3.1 - Architecture of k-NN classification over semantically secured encrypted relational data

Consider an authorized user Bob who wants to classify his query record q; q1;...;qi based onD0in C1.Theproposed PPkNN protocol mainly consists of the following two stages:

Stage1: Secure Retrieval of k-Nearest Neighbors:

In this stage, Bob initially sends his queryq (in encrypted form) to C1. After this, C1 andC2involve in a set of sub-protocols to securely retrieve (in encrypted form) the class labels corresponding tothe k-nearest neighbors of the input query q. At theend of this step, encrypted class labels of k-nearest neighbors are known only toC1.

Stage 2:Secure Computation of Majority Class:

Following from Stage 1, C1 andC2 jointly compute the class label with a majority voting among the k-nearest neighbors of q. At the end of this step, only Bob knows the class label corresponding to his input query record.

This paper is implemented in the following modules:,

- Secure Data Upload
- Query Processing
- k-NN Query Process

4.1. Secure Data Upload

An Administrator has to already register itself. An administrator can export the data to the cloud. When he upload the data, it should be encrypted before storing in to a database. There are two types of data uploaded incloud. One is the normal query process data (like voter list data), and the second one is the k-NN query process (like X and Y values). After that, an user can register to the cloud. The registered users only have permission for access the cloud data, so the unauthorized can't access the secure data from the cloud storage.

4.2. Query Processing

After the user login to access the normal query window, an user has to select the database name, table name and data owner access code from the database. This process to protect the confidentiality of the data, user's input query, and hides the data access pattern. The users input query will be encrypted and passed to the cloud database. The query can retrieve the data from the cloud and show the encrypted and decrypted data in the output window.

4.3. kNN Query Process

kNN query cannot be directly processed with the encrypted data. For that, we have to design a kNN query processing algorithm based on range queries (the PPkNN algorithm). As a result, the use of index in range query processing also enables fast processing of PPkNN queries.

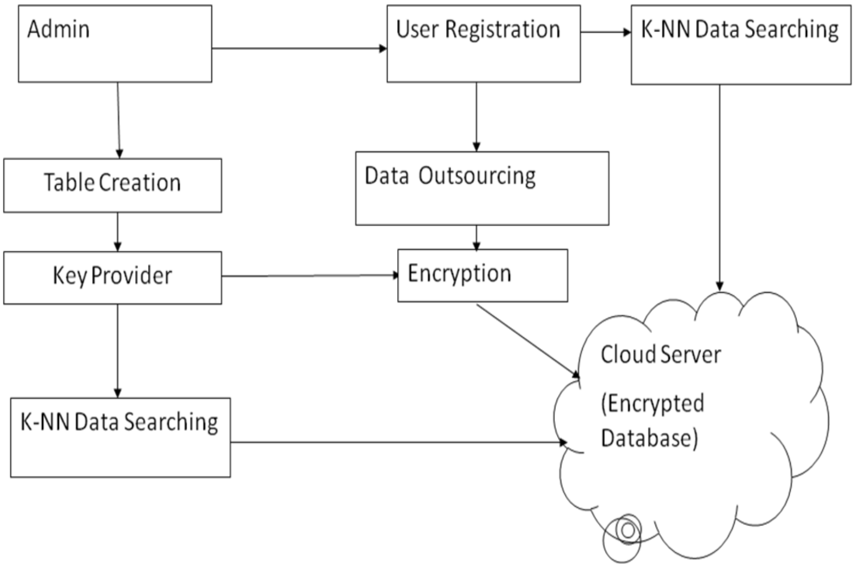


Fig 4.1. – System Architecture

The PPkNN algorithm consists of two rounds of interactions between the client and the server. The client will send the initial upper-bound range, which contains more than k points, and the initial lower-bound range, which contains less than k points, to the server. The server finds the inner range and returns to the client. The client calculates the outer range based on the inner range and sends it back to the server. The server finds the records in the outer range and sends them to the client. The client decrypts the records and finds the top range data as the final result.

V. CONCLUSION

A new PPkNN classification protocol is implemented on encrypted data in cloud. This protocol achieves the data confidentiality, input query of user, and hides access pattern of data.It protects user privacy records and is applicable to outsourced environment of database where data stays in encrypted form on third party server.

Our protocol PPk-NN protocol protects the confidentialityof the data, users input query and hides the data access patterns. In future, its performance can be improvedby providing alternative and more efficient solutions. We can also extend our research to other classification algorithms**.**

REFERENCES

1. P. Mell and T. Grance, " The NIST definition of cloud computing (draft)," NIST Special Publication, vol. 800, p. 145, 2011.
2. S. De Capitani di Vimercati, S. Foresti, and P. Samarati, " Managing and accessing data in the cloud: Privacy risks and approaches," in Proc. 7th Int. Conf. Risk Security Internet Syst., 2012, pp. 1– 9. 1272 IEEE Transactions on Knowledge and Data Engineering, VOL. 27, NO. 5, MAY 2015
3. P. Williams, R. Sion, and B. Carbunar, " Building castles out of mud: Practical access pattern privacy and correctness on untrusted storage," in Proc. 15th ACM Conf. Comput. Commun. Security, pp. 139– 148, 2008.
4. P. Paillier, " Public key cryptosystems based on composite degree residuosity classes," in Proc. 17th Int. Conf. Theory Appl. Cryptographic Techn., pp. 223– 238, 1999.
5. B. K. Samanthula, Y. Elmehdwi, and W. Jiang, " k-nearest neighbor classification over semantically secure encrypted relational data," eprint arXiv:1403.5001, 2014.
6. C. Gentry, " Fully homomorphic encryption using ideal lattices," in Proc. 41st Annu. ACM Sympos. Theory Comput., pp. 169– 178, 2009.
7. C. Gentry and S. Halevi, " Implementing gentry' s fully-homomorphic encryption scheme," in Proc. 30th Annu. Int. Conf. Theory Appl. Cryptographic Techn.: Adv. Cryptol., pp. 129– 148, 2011.
8. A. Shamir, " How to share a secret," Commun. ACM, vol. 22, pp. 612– 613, 1979.
9. D. Bogdanov, S. Laur, and J. Willemson, " Sharemind: A framework for fast privacy-preserving computations," in Proc. 13th Eur. Symp. Res. Comput. Security: Comput. Security, pp. 192– 206, 2008.
10. R. Agrawal and R. Srikant, Privacy-preserving data mining,ACM Sigmod Rec., vol.29, pp. 439– 450, 2000.

Preserved IDs for MANET's using Triple DES Algorithm

Mr. N.Kumar,
Associate Professor & HOD,
Department of Computer Science and Engineering
AKT Memorial College of Engineering and Technology

Ms. Muthupriya, Ms. S.Swarnalekha
UG Students,
Department of Computer Science and Engineering.
A.K.T.Memorial College of Engineering and Technology,

Abstract -* Data transfer rate is more in wireless network as compared to wired network .Wireless network gives more advantageous because its support feature such as versatility, portability, open medium, simple to design. MANETs and WSN are the most common forms of Wireless media. In MANETs nodes are deployed or distributed in Ad-hoc way and they are communicating or exchange message using wireless Transmission. Security is a measure concern in Mobile Ad-hoc Network because MANETs having wide distribution of node & open medium it becomes vulnerable to malicious attackers very fast. Now we recommend and execute more powerful and secure intrusion detection system named Improved EAACK designed for MANETs. Improved EAACK schema uses concepts such as hybrid cryptography & bouncing theory for reducing network overhead & removing unwanted node and forward traffic through a precise location. Performance is measured using Packet Delivery Ratio & Routing Overhead.

Keywords - Enhanced Adaptive Acknowledgment (EAACK); Mobile Ad hoc Network (MANET); Packet Delivery Ratio (PDR); Received Signal Strength (RSS); Rivest Shamir Adleman (RSA).

I.INTRODUCTION

MANETs is very Successive, attractive, and pervasive technology in wireless network. The advancement of wireless system is additionally requesting from a decade ago. Nodes a network sending or passing message to next node it forms a temporary ad hoc network of some node. Maintaining mobility is important task done by Manets. MANETS are much more susceptible different type of attack because provide distributed architecture, volatile network topology, limited bandwidth. of single hop or multihope. in single hope all the node in the defined coverage area. And if there is intermediate node used for communication between two nodes is called multihop network [7], [8]. IN MANETs there are two types of attack possible one is active attack and another is Passive attack. Number of downsides for expelling these disadvantages in this paper we anticipated new framework i.e Improved EAACK.

MANET is used in emergency requirements because it allows easy deployment, minimal configuration, low cost. It has restricted battery power and resources.

II. BACKGROUND

Providing security is very challenging task in MANETs. There are numerous IDS has been produced for giving security. In this area, we fundamentally portray three exhibited approaches namely, Watchdog, TWOACK, and Adaptive Acknowledgment (AACK).

A. Watchdog

Marti anticipated method watchdog for detecting misbehaving node which is Unsafe for network. It operates in two phase first is Watchdog and second is path rater.It uses its next hops transmission for detecting the misbehaving attack which is present in the network. It increases its failure counter if next node fails to transfer packet within time limit.Whenever a node's failure counter surpasses a predefined threshold, the Watchdog node reports it as misbehaving. The path rater technique used for in any future route selections for avoiding the use of malicious node in the network. Shortcoming of the watchdog algorithm is

1) Ambiguous collisions.
2) Receiver collisions.
3) Limited transmission power.
4) False misbehavior report.
5) Collusion.
6) Partial dropping.

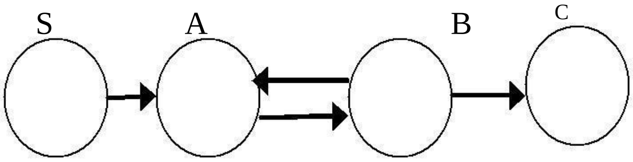


Figure 1: Watchdog schema

An above figure shows the how operation take in watchdog.

B. TWOACK

Some of the drawbacks which are present in previous IDS, such as limited transmission power and receiver collision to avoid these limitation and to increase the performance of network TWOACK schema is proposed .It uses three consecutive node to transfer packet from source to destination.

C. AACK

It consist the combination of TWOACK and TACK. It transfer packet from the first node to last node. Destination node gives feedback to first node. It gives the good result than the watchdog and TWOACK. But drawbacks of the AACK are it is not suitable for when there is number node in the network is large.

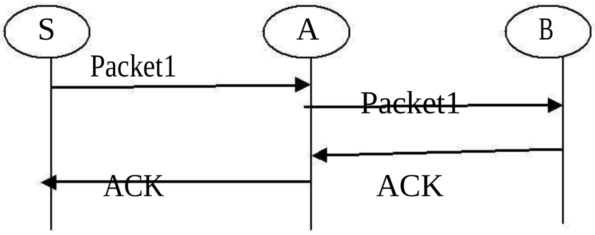


Figure 2: ACK scheme

III. LITERATURE REVIEW

1) Watchdog & pathrater

Watchdog and Pathrater is designed by S. Marti, T. J. Giuli It was the traditional IDS system for MANETs. It has number of drawbacks which have been studied in previous section.

2) EAACK

N.kang, E.Shakshuki and T.Sheltami develop new IDS for MANETs. It overcomes all the drawbacks of previous IDS.It use AODV protocol and useful to detect wormhole attack, misbehaving attack ,Gray hole attack which may be present in the network [14].

3) IEAACK

P. Joshi, P. Nande, A. Pawar, P. Shinde, and R. Umbrae, develop more powerful secure intrusion detection system called IEAACK which remove drawbacks of all previous intrusion detection system. it uses AODV protocol ,it detect all malicious node ,it detect all types of attack prevent them.[1].

4) Hybrid cryptography

B.Suruthi and N. V. Rajeesh Kumar, [5].It uses new technique for balancing load on network called Hybrid cryptography it also increases the performance of network. It uses RSA, AES key for encryption and it uses zone routing protocol for discovering path from source to destination.

IV. SYSTEM DESCRIPTION

A. ACK

It is circular acknowledgment schema packet is send from source to destination. Then destination sends an acknowledgement packet to source within fix time otherwise again same packet is send once more.

B. S-ACK

It uses three following nodes for detecting misbehaving node which attacks the system .Source node send the packet to destination node then it gives acknowledgment back to source node. for sending S-ACK packet to source node third node is used. It removes limitation of TWO-ACK schema. It urgently create misbehavior report, it is primary step of misbehavior report authentication. Main purpose of this algorithm is detecting the mischievous nodes in the network channel.

C. MRA

The source will check with the destination whether the destination node have received the dropped packet or not. source node send misbehavior to MRA node .Then MRA node send same packet which was being sent but at this time it uses a different route for sending packet. for sending packet it searches path using it own local knowledge base table, it contain information about route path selection. Then it checks the result if the same packet is reach target node for early time then misbehavior report generated is correct. On other hand if same packet is already designated then false report is generated and which node generate this report marked as folksy Node or misbehaving node or malicious node and removing these node for securing the network. All the above three are the part of EAACK algorithm.

V. SYSTEM ARCITECTURE

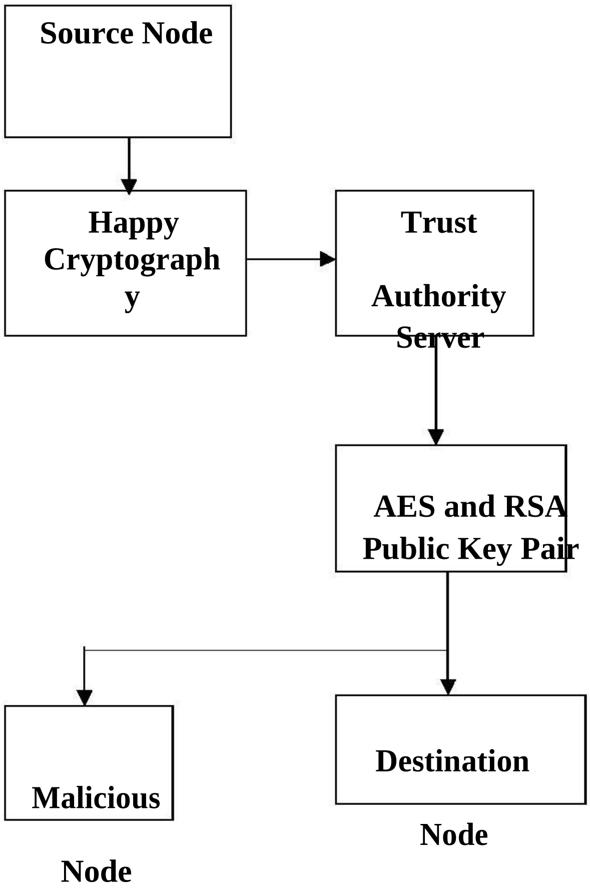


Figure 3: Proposed System Architecture

Hybrid cryptography technique use AES and RSA Public Key Pair to send data from source to destination. AES algorithm is used for encrypting text which is decrypted by same key .It is as a form of symmetric block cipher. it is connected with the TA to ensure that symmetric keys are established.

Figure 1: Performance analysis (scenario1)

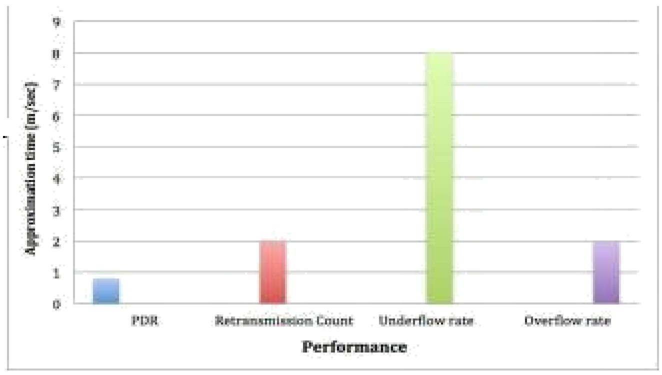
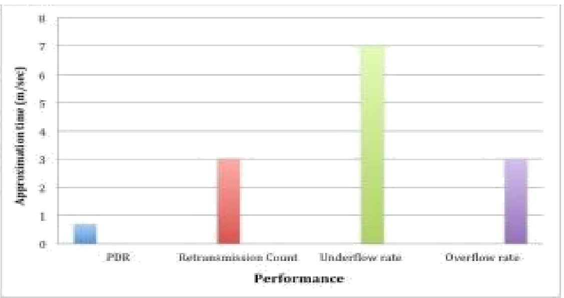


Figure 2: Performance analysis(scenario 2)



VI.COCLUSION AND FUTURE WORK

Packet drop detection is important for providing security to MANET. It uses acknowledgement schema such as TWO ACK,ACK,AACK,EAACK to avoid the defect. EAACK gives better performance then other schema. It uses digital signature to avoid routing overhead. Therefore in this paper we proposed hybrid cryptography to reduce routing overhead by detecting malicious path. Using shared key source node and destination node authenticate to transfer data packets.

Remote Data Integrity Checking with Preserving Data for Cloud Storage

Mr. V. Aravindsai, Mr. S.Arunkumar, Mr. V.Vignesh
UG Students
MRK Institute of Technology, Kattumannarkoil

Abstract - Using Cloud Storage, users can tenuously store their data and enjoy the on-demand great quality applications and facilities from a shared pool of configurable computing resources, without the problem of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained dividing resources. From users’ perspective, including both individuals and IT systems, storing data remotely into the cloud in a flexible on-demand manner brings tempting benefits: relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc. . To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to capably audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should take in no new vulnerabilities towards user data privacy. In this project, utilize and uniquely combine the public auditing protocols with double encryption approach to achieve the privacy-preserving public cloud data auditing system, which meets all integrity checking without any leakage of data. To support efficient handling of multiple auditing tasks, we further explore the technique of online signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. We can implement double encryption algorithm to encrypt the data twice and stored cloud server.

1. INTRODUCTION

1.1 General

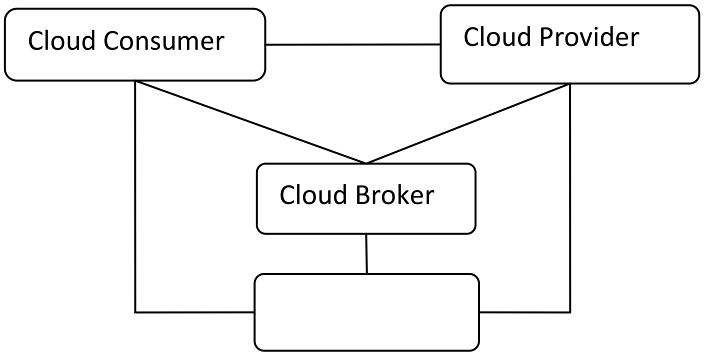
While the storage of corporate data on remote servers is not a new development, current expansion of cloud computing justifies a more careful look at its actual consequences involving privacy and confidentiality issues. As users no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted. In particular, simply downloading all the data for its integrity verification is not a practical solution due to the expensiveness in I/O and transmission cost across the network. Besides, it is often insufficient to detect the data corruption only when accessing the data, as it does not give users correctness assurance for those un-accessed data and might be too late to recover the data loss or damage. To fully ensure the data integrity and save the cloud users' computation resources as well as online burden, it is of critical importance to enable public auditing service for cloud data storage, so that users may resort to an independent third party auditor (TPA) to audit the outsourced data when needed. The TPA, who has expertise and capabilities that users do not, can periodically check the integrity of all the data stored in the cloud on behalf of the users, which provides a much more easier and affordable way for the users to ensure their storage correctness in the cloud. In a word, enabling public auditing services will play an important role for this nascent cloud economy to become fully established; where users will need ways to assess risk and gain trust in the cloud.

1.2 CLOUD COMPUTING

Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly. It is a practical approach to experience direct cost benefits and it has the potential to transform a data center from a capital-intensive set up to a variable priced environment. The idea of cloud computing is based on a very fundamental principles of reusability of IT capabilities. The difference that cloud computing brings compared to traditional concepts of "grid computing", "distributed computing", "utility computing", or "autonomic computing" is to broaden horizons across organizational boundaries. Forrester [1] defines cloud computing as: "A pool of abstracted, highly scalable, and managed compute infrastructure capable of hosting end customer applications and billed by consumption". It is a technology that uses the internet and central remote servers to maintain data and applications and allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing data storage, processing and bandwidth. Cloud computing examples are Yahoo email, Gmail, or Hotmail.

1.3 ARCHITECTURE

Figure 1.1 Architecture of cloud computing



1.3.1 Cloud Provider

A person, organization, or entity responsible for making a service available to interested parties. A Cloud Provider acquires and manages the computing infrastructure required for providing the services, runs the cloud software that provides the services, and makes arrangement to deliver the cloud services to the Cloud Consumers through network access

1.3.2 Cloud Consumer

"A person or organization that maintains a business relationship with, and uses service from, Cloud Providers. A cloud consumer browses the service catalog from a cloud provider, requests the appropriate service, sets up service contracts with the cloud provider, and uses the service. The cloud consumer may be billed for the service provisioned, and needs to arrange payments accordingly."

1.3.3 Cloud Auditor

A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation. A cloud auditor is a party that can perform an independent examination of cloud service controls with the intent to express an opinion thereon. Audits are performed to verify conformance to standards through review of objective evidence. A cloud auditor can evaluate the services provided by a cloud provider in terms of security controls, privacy impact, performance, etc.

1.3.4 Cloud Broker

"As cloud computing evolves, the integration of cloud services can be too complex for cloud consumers to manage. A cloud consumer may request cloud services from a cloud broker, instead of contacting a cloud provider directly. Hence the broker is an entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers." Brokers provide three different types of services to the Cloud Consumer.

1.4 SERVICE MODELS OF CLOUD

Cloud Providers offer services that can be grouped into three categories in figure 1.2.

- Software as a Service (SaaS)
- Platform as a Service (Paas)
- Infrastructure as a Service (Iaas)

1.4.1 Software as a Service

In this model, a complete application is offered to the customer, as a service on demand. A single instance of the service runs on the cloud & multiple end users are serviced. On the customers‟ side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted & maintained. Today SaaS is offered by companies such as Google, Salesforce, Microsoft, Zoho, etc.

1.4.2 Platform as a Service

Here, a layer of software, or development environment is encapsulated & offered as a service, upon which other higher levels of service can be built. The customer has the freedom to build his own applications, which run on the provider‟s infrastructure. To meet manageability and scalability requirements of the applications, PaaS providers offer a predefined combination of OS and application servers, such as LAMP platform (Linux, Apache, MySql and PHP), restricted J2EE, Ruby etc. Google‟s App Engine, Force.com, etc are some of the popular PaaS examples.

1.4.3 Infrastructure as a Service

IaaS provides basic storage and computing capabilities as standardized services over the network. Servers, storage systems, networking equipment, data centre space etc. are pooled and made available to handle workloads. The customer would typically deploy his own software on the infrastructure. Some common examples are Amazon, GoGrid, 3 Tera, etc.

1.5 DEPLOYMENT MODELS OF CLOUD

Enterprises can choose to deploy applications on Public, Private or Hybrid clouds. Cloud Integrators can play a vital part in determining the right cloud path for each organization.

1.5.1 Public Cloud

Public clouds are owned and operated by third parties; they deliver superior economies of scale to customers, as the infrastructure costs are spread among a mix of users, giving each individual client an attractive low-cost, “Pay-as-you-go” model. All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. These are managed and supported by the cloud provider. One of the advantages of a Public cloud is that they may be larger than an enterprises cloud, thus providing the ability to scale seamlessly, on demand.

1.5.2 Private Cloud

Private clouds are built exclusively for a single enterprise. They aim to address concerns on data security and offer greater control, which is typically lacking in a public cloud. There are two variations to a private cloud:

- On-premise Private Cloud
- Externally hosted Private Cloud

1.5.2.1 On-premise Private Cloud

On-premise private clouds, also known as internal clouds are hosted within one's own data center. This model provides a more standardized process and protection, but is limited in aspects of size and scalability. IT departments would also need to incur the capital and operational costs for the physical resources. This is best suited for applications which require complete control and configurability of the infrastructure and security.

1.5.3 Hybrid Cloud

Hybrid Clouds combine both public and private cloud models. With a Hybrid Cloud, service providers can utilize 3rd party Cloud Providers in a full or partial manner thus increasing the flexibility of computing. The Hybrid cloud environment is capable of providing on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload

2. SYSTEM ANALYSIS

2.1. Existing System

While cloud computing makes various advantages, it can be mentioned in chapter 1 and challenging security threats toward users' outsourced data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing is actually relinquishing user's ultimate control over the fate of their data. As a result, the correctness of the data in the cloud is being put at risk due to the following reasons First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity. Examples of outages and security breaches of noteworthy cloud services appear from time to time. Second, there do exist various motivations for CSP to behave unfaithfully toward the cloud users regarding their outsourced data status. CSP might reclaim storage for monetary reasons by discarding data that have not been or are rarely accessed, or even hide data loss incidents to maintain a reputation. In short, although outsourcing data to the cloud is economically attractive for long-term large-scale storage, it does not immediately offer any guarantee on data integrity and availability. This problem, if not properly addressed, may impede the success of cloud architecture. As users no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted. In particular, simply downloading all the data for its integrity verification is not a practical solution due to the expensiveness in I/O and transmission cost across the network. Besides, it is often insufficient to detect the data corruption only when accessing the data, as it does not give users [2] correctness assurance for those un-accessed data and might be too late to recover the data loss or damage.

2.1.1 Watermarking Scheme

And implement the system to provide water marking process, to store the data or images in the cloud server by assigning the public key, and this key and watermarking images are sent to third party and third party have complete authority to check the key and sent it to the server, and there Third Party Auditor must have a public key whenever the data to be retrieved. In the watermarking process, the security level is very high so the data or images cannot be identified by the attackers in the cloud and also use Compression technique for watermark image to reduce communication overhead. The main elements in watermarking process: an embedded, a communication channel and a detector. Watermark information is embedded into original image itself, and it is performed in the encryption process for making security on original information. Embedded is similar to encryption process which is used to change content into another format with the help of the secret key. Detector process is also similar to decryption process which is used to perform reverse process of encryption. The watermark information is embedded within the original image before the watermarked image is transmitted over the communication channel, so that the watermark image can be detected at the receiving end.

2.1.2 One Ring To Rule Them All (Oruta) Scheme:

Then implemented ORUTA that include a privacy preserving public auditing mechanism for shared data in an untrusted cloud. In Oruta, utilize ring signatures to construct homomorphic authenticators, so that the third party auditor is able to verify the integrity of shared data for a group of users without retrieving the entire data — while the identity of the signer on each block in shared data is kept private from the TPA. In addition, extend the mechanism to support batch auditing, which can audit multiple shared data simultaneously in a single auditing task. Meanwhile, Oruta continues to use random masking to support data privacy during public auditing, and leverage index hash tables to support fully dynamic operations on shared data. A dynamic operation indicates an insert, delete or update operation on a single block in shared data. In this paper, we only consider how to audit the integrity of shared data in the cloud with static groups. It means the group is pre-defined before shared data is created in the cloud and the membership of users in the group is not changed during data sharing. The original user is responsible for deciding who is able to share her data before outsourcing data to the cloud.

2.1.3 Disadvantages

- Leak users' data to external auditor
- Can extract the original data of a user during the auditing process
- Existing system provide insecurity scheme for data auditing
- Provide Computational overheads

2.2 Proposed System

The system model in this project involves three parties: the cloud server, a group of users and a public verifier. There are two types of users in a group: the original user and a number of group users. The original user initially creates shared data in the cloud, and shares it with group users. Both the original user and group users are members of the group. Every member of the group is allowed to access and modify shared data. Shared data and its verification metadata (i.e. signatures) are both stored in the cloud server. A public verifier, such as a third-party auditor (TPA) providing expert data auditing services or a data user outside the group intending to utilize shared data, is able to publicly verify the integrity of shared data stored in the cloud server. When a public verifier wishes to check the integrity of shared data, it first sends an auditing challenge to the cloud server. After receiving the auditing challenge, the cloud server responds to the public verifier with an auditing proof of the possession of shared data. Then, this public verifier checks the correctness of the entire data by verifying the correctness of the auditing proof. Essentially, the process of public auditing is a challenge and-response protocol between a public verifier and the cloud server.

Public Auditing A public verifier is able to publicly verify the integrity of shared data without retrieving the entire data from the cloud.

Correctness A public verifier is able to correctly verify shared data integrity.

Unforgetability Only a user in the group can generate valid verification metadata (i.e., signatures) on shared data.

Identity Privacy A public verifier cannot distinguish the identity of the signer on each block in shared data during the process of auditing.

With cloud computing and storage, users are able to access and to share resources offered by cloud service providers at a lower marginal cost. It is routine for users to leverage cloud storage services to share data with others in a group, as data sharing becomes standard feature in most cloud storage offerings, including Dropbox, iCloud and Google Drive. The integrity of data in cloud storage, however, is subject to skepticism and scrutiny, as data stored in the cloud can easily be lost or corrupted due to the inevitable hardware/software failures and human errors. The traditional approach for checking data correctness is to retrieve the entire data from the cloud, and then verify data integrity by checking the correctness of signatures or hash values of the entire data. Certainly, this conventional approach able to successfully check the correctness of cloud data. However, the efficiency of using this traditional approach on cloud data is in doubt. The main reason is that the size of cloud data is large in general. Downloading the entire cloud data to verify data integrity will cost or even waste user’s amounts of computation and communication resources, especially when data have been corrupted in the cloud. Recently, many mechanisms have been proposed to allow not only a data owner itself but also a public verifier to efficiently perform integrity checking without downloading the entire data from the cloud, which is referred to as public auditing. In these mechanisms, data is divided into many small blocks, where each block is independently signed by the owner; and a random combination of all the blocks instead of the whole data is retrieved during integrity checking. A public verifier could be a data user (e.g. researcher) who would like to utilize the owner’s data via the cloud or a third-party auditor (TPA) who can provide expert integrity checking service. In this proposed system we can implement Merkle Hash Tree to spilt the files into various parts and to provide double encryption concept to encrypt the data first at owner side and again encrypt the data based on TPA provided keys. Finally provide batch auditing schemes to perform multiple tasks at a time and user level privacy can be implemented to share the data without any leakages.

2.2.1 Advantages

- Improved Public auditability and privacy-preserving
- Fully data dynamics
- Fast auditing and low performance protocols
- End device friendliness

III. CONCLUSION

Cloud computing securities are discussed and analyzed in previous study. In this project, some of the privacy threats are addressed and the techniques to overcome them are surveyed. While some approaches utilized traditional cryptographic methods to achieve privacy, some other approaches kept them away and focused on alternate methodologies in achieving privacy. Also, approaches to preserve privacy at the time of public auditing are also discussed. Thus, to conclude it is necessary that every cloud user must be guaranteed that his data is stored, processed, accessed and audited in a secured manner at any time. Data freshness is essential to protect against misconfiguration errors or rollbacks caused intentionally and can develop an authenticated file system that supports the migration of an enterprise-class distributed file system into the cloud efficiently, transparently and in a scalable manner. It’s authenticated in the sense that enables an enterprise tenant to verify the freshness of retrieved data while performing the file system operations. The user must be given complete access control over the published data. Also, powerful security mechanisms must always supplement every cloud application. Attaining all these would end up in achieving the long dreamt vision of secured Cloud Computing in the nearest future.

IV. FUTURE ENHANCEMENT

In future, this proposed model could be used to get the secure cloud computing environment which would be a great enhancement in the privacy preservation. And implement various protocols to improve the security of the system.

REFERENCES

1. G. Ateniese, A. Faonio, and S. Kamara, “Leakage-resilient identification schemes from zero-knowledge proofs of storage,” in IMA Inte. Conf. Cryptography and Coding, 2015, pp. 311–328.

2. Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," IEEE Trans. Parallel Distrib.Syst., doi.10.1109/TPDS. 2015.2506573.
3. Z. Hao, S. Zhong, and N. Yu, "A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability," IEEE Trans. Knowl.Data Eng., vol.23, no.9, pp.1432-1437, 2011.
4. H. Liu, L. Chen, Z. Davar, and M. Pour, "Insecurity of an efficient privacy-preserving public auditing scheme for cloud data storage," J. Universal Comput.Sci., vol. 21, no. 3, pp. 473–482, 2015.
5. J. K. Liu, M. H. Au, X. Huang, R. Lu, and J. Li, "Fine-grained twofactor access control for web-Based cloud computing services," IEEE Trans. Inf. Forens. Security, vol. 11, no. 3, pp. 484–497, 2016.
6. F. Seb´e, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J. J. Quisquater, "Efficient remote data possession checking in critical information infrastructures," IEEE Trans. Knowl. Data Eng., vol. 20, no.8, pp. 1034–1038, 2008
7. C. Wang, Q. Wang, S. C, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62, no. 2, pp. 362–375, 2013.
8. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proc. IEEE Int. Conf. Comput.Commun. (INFOCOM), 2010, pp. 1–9.
9. Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 2, pp. 340-352, 2015.
10. L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and Z. Dong, "Round-efficient and sender-unrestricted dynamic group key agreement protocol for secure group communications," IEEE Trans. Inf. Forensic Security, vol. 10, no. 11, pp. 2352-2364, 2015.

Sentimental Analysis of the GST of Economy 2017 India

Ms.P.Kuzhali, Ms. M.B Saraswathy, Ms. G.Sasikala
UG Students,
Department of Information Technology
Anand Institute of Higher Technology

Mr. M.V Balaganesh
Assistant Professor-I
Anand Institute of Higher Technology

Abstract - In crowdfunding, the sentimental factor of the text description may impact the backers, investment intention on the project. The authors study the textual description from the sentimental aspect on the pledge results by employing text mining. Although there have been many approaches to analyzing sentiments on twitter but extremely few has been found which also consider region wise classification of the sentiment. Also, recently in India there has been a drastic change due to GST of the economy. Our aim is to mine this product wise and conclude whether product wise classification can give us more specification about the GST.

Index Terms - twitter, sentiment analysis, region wise, SVM.

I. INTRODUCTION

In the past decade, new forms of communication, such as micro blogging and text messaging have emerged and become ubiquitous. Twitter has a major role to play when it comes to our lives today. Not just because it is a medium to connect but simply because it is a place where people can openly express our opinion through this micro-blogging website. It is extremely useful to openly share your opinion and directly communicate with the who's who of your field that is the people who concerned with the topic of our concern. It is also advantageous when it comes to mining the opinions because it as 140 word limit so the thoughts are more precise as compared to other social media websites. Also, with the growing popularity of twitter their are more and more people joining this form and hence creating a platform for interest of researchers. It has been reported that there are 317 million active twitter uers monthly which is a greater number to create a platform for research and opinion mining.

GST that is goods and service tax is the new buzz across the country today. Everyone is interested in knowing the impact that the new GST law will have in their day to day life and also to our economy. GST is being widely debated by economists, business leaders, industrialists, tax professionals and the general public at large. It is being considered as the biggest tax reform in India's 70 year history as an independent nation.

Recently, by our honourable prime minister an important decision was taken to stop the use of 500 and1000 rupee notes in the Indian market to eradicate the use of the black money. It is very positive move but at the same time has taken a toll on the common man who has to stand at long queues outside banks, ATM's and post offices to exchange the old currency with the new one with a lot of do's and don'ts introduced as a part of the policy. It has received a lot of positive and negative feedback. The aim is to analyze the sentiments of people in various parts of Indianan this regard through a new approach at the same time comparing it with the previously existing methods.

Due to twitter's growing popularity there has been a lot of work varied on twitter sentiment analysis. The attempt is to provide a novel approach which uses to filter tweets product wise and at the same time compare it in terms of accuracy and efficiency. A comparison has been made between both the popular approaches of naïve Bayes classify and SVM classifier, which is used to give the accurate results. It was useful to understand separatly the kind of sentiment each part of India has expressed towards the initiative.

II. RELATED WORKS

Social media has been explored to estimate the popularity of politicians, sentiments of general public towards some recently introduced policy maybe budget, tax reforms etc., to find out the sentiments of social media users .Social networking sites have also been used to compare people's political preferences expressed online with those observed by elections. Social media can be analyzed on daily or hourly basis during an electoral campaign so as to get a detailed insight into emotions of voters. It is possible to track in real-time trends and capture any sudden change by monitoring and analyzing the conversation on social networking sites and get the public opinion well before declaration of results of polls. There are few studies that claim that analyzing social media allows a reliable forecast of the final result. In a study by researchers, it has been stated that the number of times a candidate is mentioned in blog posts is a good predictor of electoral success and can achieve better predictions than election polls. There are claims by some researchers that more the number of facebook supporters an electoral candidate has, better are the chances to win .On similar lines the authors, compared party pointed out on Twitter with the results of the 2009 German election and discussed that the relative number of tweets related to each party is a good predictor of its vote share. There stands a better way to analyze tweets such that not just the count or mention of party name or candidate name is considered but the sentiment attached in tweets are also analyzed. A sentiment classifier based on lexical induction has been built and correlations between several polls conducted during the 2008 presidential election and the content of wall posts available on Facebook has been found. There are other studies that show similar results displaying correlation between Obama's approval rate and the sentiment expressed by Twitter users. For predicting the results of both the 2011 and the 2012 legislative elections in the Netherlands, sentiment analysis of tweets proved to perform quite well.

III. DATA COLLECTION AND PREPROCESSING

Twitter has been used to keep track of temporal nature of elections. The sentiments keep on changing based on some announcement or news by political parties. By creating a twitter API, 5,000 tweets have been collected and examined. The tweets published on Twitter's public message board one day prior to the GST implementation announcement and on the day of announcement (30-June 2017 and 1-July 2017), have been collected. The tweets comprised of useful information related to GST besides special characters, punctuation marks and score. The data collected hence has been cleaned so as to remove punctuation symbols, special characters. All tweets have been converted to lowercase and finally a word corpus has been generated.

Feature Extraction: The preprocessed dataset has many distinctive properties. In the feature extraction method, we extract the aspects from the processed dataset. Later this aspect are used to compute the positive and negative polarity in a sentence which is useful for determining the opinion of the individuals using models like unigram, bigram. Machine learning techniques require representing the key features of text or documents for processing. These key features are considered as feature vectors which are used for the classification task. Some examples features that have been reported in literature are:

1. Words and Their Frequencies: Unigrams, bigrams and n-gram models with their frequency counts are considered as features. There has been more research on using word presence rather than frequencies to better describe this feature. showed better results by using presence instead of frequencies.

2. Parts Of Speech Tags: Parts of speech like adjectives, adverbs and of verbs and nouns are good indicators of subjectivity and sentiment. We can generate syntactic dependency patterns by parsing or dependency trees.

3. Opinion Words And Phrases: Apart from specific words, some phrases and idioms which convey sentiments can be used as features. e.g. cost someone an arm and leg.

4. Position Of Terms: The position of a term with in a text can affect on how much the term makes difference in overall sentiment of the text.

5. Negation: Negation is an important but difficult feature to interpret. The presence of a negation usually changes the polarity of the opinion..

IV. APPROACHES FOR SENTIMENTAL ANALYSIS

There are mainly two techniques for sentiment analysis for the twitter data Machine Learning Approaches Machine learning based approach uses classification technique to classify text into classes. There are mainly two types of machine learning techniques.

Unsupervised learning: It does not consist of a category and they do not provide with the correct targets at all and therefore rely on clustering. .

Supervised learning: It is based on labeled dataset and thus the labels are provided to the model during the process. These labeled dataset are trained to get meaningful outputs when encountered during decision making. The success of both this learning methods is mainly depends on the selection and extraction of the specific set of features used to detect sentiment. The machine learning approach applicable to sentiment analysis mainly belongs to supervised classification. In a machine learning techniques, two sets of data are needed:

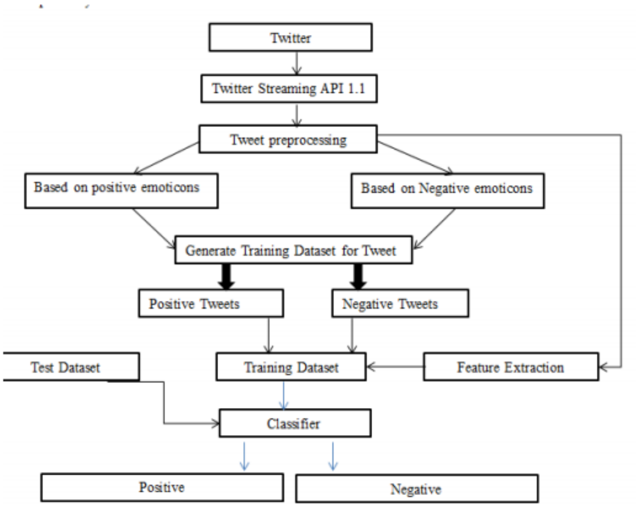
1. Training Set

2. Test Set

A number of machine learning techniques have been formulated to classify the tweets into classes. Machine learning techniques like Naive Bayes (NB), maximum entropy (ME), and support vector machines (SVM) have achieved great success in sentiment analysis. Machine learning starts with collecting training dataset. Nextly we train a classifier on the training data. Once a supervised classification technique is selected, an important decision to make is to select feature. They can tell us how documents are represented. The most commonly used features in sentiment classification are Term presence and their frequency

- Part of speech information
- Negations
- Opinion words and phrases
- Support vector machine

Support vector machine analyzes the data, define the decision boundaries and uses the kernels for computation which are performed in input space. The input data are two sets of vectors of size m each. Then every data which represented as a vector is classified into a class. Nextly we find a margin between the two classes that is far from any document. The distance defines the margin of the classifier, maximizing the margin reduces indecisive decisions. SVM also supports classification and regression which are useful for statistical learning theory and it also helps recognizing the factors precisely, that needs to be taken into account, to understand it successfully.



V. CONCLUSION

The increasing number of social media websites by Internet users has raised the interest about the opportunity to understand the relation between people's preferences and actual political behaviour. This study focuses on the question that whether the data from social networking sites can be utilized to interpret the attitude of citizens of a nation towards various policies. We analyzed 5,000 twitter messages mentioning keyword viz. "GST" for two days, viz. one day prior to announcement and on the day of announcement We have observed that twitter is very commonly being used as a platform for deliberation by citizens of India. It has been concluded that social media is a powerful and reliable source of public opinion as far as a nation like India is concerned. The discussions on twitter are equivalent to traditional discussions and are capable enough to give a fair idea of emotions of general public. We have done sentiment analysis of emotions of people which shows people's acceptance for GST but with too much of anticipation feeling. In future, we plan to convert this analysis in real time corresponding to tweets arriving on temporal scale. Also we can geographically divide and analyze the tweets.

Analyses was done on this labeled datasets using various feature extraction technique. We used the framework where the preprocessor is applied to the raw sentences which make it more appropriate to understand. we have analysed that **30%** of people have positive opinion on GST, **20%** are neutral opinion, remaining **50%** of people are not accepted i.e., negative thoughts about GST

REFERENCES

1. Ve´ronis J. Citations dans la presse et re´sultats du premier tour de la pre´sidentielle, 2007.
2. Williams C, Gulati G. What is a social network worth? Facebook and vote share in the presidential primaries. Boston, MA: Annual Meeting of the American Political Science Association, 2008, 1-17.
3. Tumasjan A, Sprenger TO, Philipp GS, Welpe IM. Predicting elections with twitter: What 140 characters reveal about political sentiment. Social Science Computer Review, 2011; 29:402-418.
4. Chung J, Mustafaraj E. Can collective sentiment expressed on twitter predict political elections? Proceedings of the Twenty-Fifth AAAI Conference on Artificial Intelligence, San Francisco, CA, 2011.
5. Wei wang ,Kevin zhu, Hongwei wang, Yen-chun Jim Wu "The impact of sentiment orientations on successful crowdfunding compaings through text analytics"(2017) .
6. Falguni Gupta , Swati Singal "Sentiment Analysis Of The Demonitization Of Economy 2016 India,Regionwise" (2017).
7. G. Carenini, R. T. Ng, and E. Zwart"Multi -Document Summarization of Product Reviews"(2012)
8. Lu lin , Jianxin li, Richong Zhang , Weiren Yu , Chenggen Sun "Opinion Mining and Sentiment Analysis in Social Networks: A Retweeting Structure-Aware Approach" (2015).
9. Ghose and P. G. Ipeirotis "Estimating The Helpfulness And Economic Impact Of Product Reviews: Mining Text And Reviewer Characteristics" (2011).
10. Wei Yen Chong , Bhawani Selvaretnam , Lay-Ki Soon "Natural Language Processing For Sentimental Analysis: An Exploratory Analysis On Tweets (2014).

Voice Command Execution with Speech Recognition and Synthesizer

Ms. G.Kowsalya, Ms. E.Parameshwari, Ms. D.Pavithra
UG Students,
AKTMCET, Kallakurichi

Abstract—**Recurrent neural network language models (RNNLMs) are becoming increasingly popular for a range of applications including automatic speech recognition. An important issue that limits their possible application areas is the computational cost incurred in training and evaluation. This paper describes a series of new efficiency improving approaches that allows RNNLMs to be more efficiently trained on graphics processing units (GPUs) and evaluated on CPUs. First, a modified RNNLM architecture with a nonclass-based, full output layer structure (F-RNNLM) is proposed. This modified architecture facilitates a novel spliced sentence bunch mode parallelization of F-RNNLM training using large quantities of data on a GPU. Second, two efficient RNNLM training criteria based on variance regularization and noise contrastive estimation are explored to specifically reduce the computation associated with the RNNLM output layer softmax normalisation term. Finally, a pipelined training algorithm utilizing multiple GPUs is also used to further improve the training speed. Initially, RNNLMs were trained on a moderate dataset with 20M words from a large vocabulary conversational telephone speech recognition task. The training time of RNNLM is reduced by up to a factor of 53 on a single GPU over the standard CPU-based RNNLM toolkit. A 56 times speed up in test time evaluation on a CPU was obtained over the baseline F-RNNLMs. Consistent improvements in both recognition accuracy and perplexity were also obtained over C-RNNLMs. Experiments on Google's one billion corpus also reveals that the training of RNNLM scales well.**

Index Terms—**Estimation, GPU, language models, noise contrastive, pipelined training, recurrent neural network, speech recognition, variance regularisation.**

Load Balancer to Achieve Green Cloud Computing

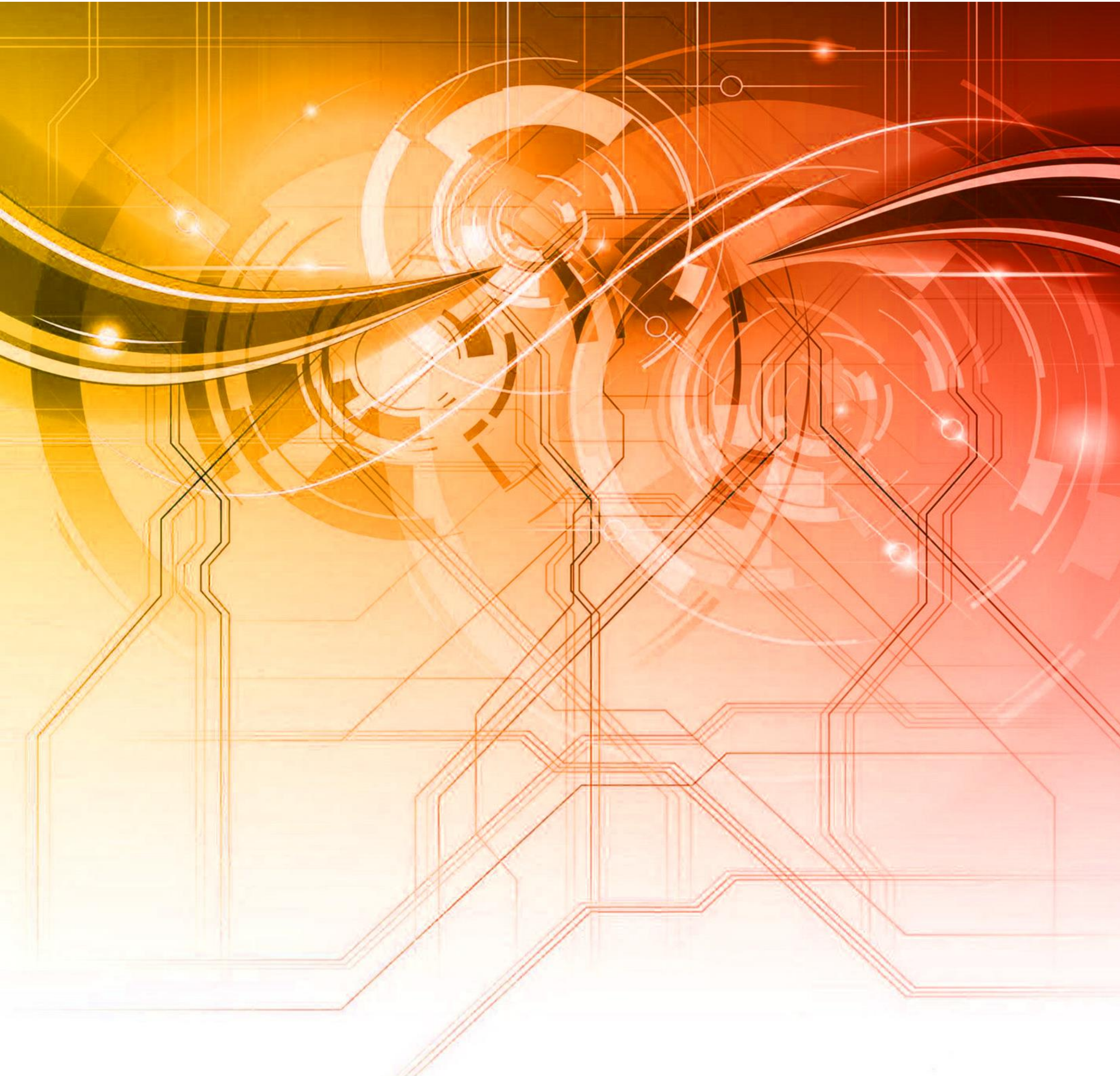
Ms. M.Malathi, Ms. C.Subhalakshmi
UG Students,
Department of Computer Science and Engineering
AKT Memorial College of Engineering and Technology

Mr. J.Raja
Assistant Professor,
Department of Computer Science and Engineering,
AKT Memorial College of Engineering and Technology

Abstract - It is proposed on load balancing. Here we both well as dynamic based In a distributed system, from the starting days onwards distribution of load among servers becomes a serious problem in the commercial Internet. The entire single application oriented server has to engage the entire amount algorithms and their performances are compared with all other existing scheme. This paper also brings connectivity on green computing with cloud load balancers. By cloud computing we can attain multi tenancy and dynamic resource handling which automatically co2 emission from servers. Without the facility of sharing single resources among thousands of peoples, green computing is not possible. So the nature of cloud load balancer and green computing was illustrated here.

Index Terms - Distributed system, Load Balancer, Load balancing algorithms, Resource provisioning.

WITH BEST COMPLIMENTS FROM



St. Anne's College of Engineering and Technology,
Anguchettypalayam, Panruti - 607 106,
Cuddalore Dt.
www.stannescet.ac.in
stannescet@gmail.com
04142 - 241661, 242661

ISBN 978-93-5254-811-8
9 789352 548118 >