TUNNEL FOLLOWER
AN AUTONOMOUS ROBOT

Varshini.B[#1]

[#1]*CSE IIIyr, SKR Engineering College*

***Abstract*--The hectic tunnel follower is an autonomous robot, is used to follow the path of the tunnel where human can't able to enter. It deals with pit and obstacle avoider robot method. Pit and obstacle avoider robot will detect the pit and the object round it. It avoids the absence of the surface and the obstacle that appears in its path. The camera that fixed in the robot is used to gatherthe live information about the path. It transfers the continuous information about the environment where the robot is present. The XBEE module is used to control the movement of the robot wirelessly. It can able to pass the information at longer distance. This robot which makes the human task easier and it also makes us to be updated with the information. It works mainly by the arduino microcontroller with the pin ATmega328. The sensors that fixed in the robot will have contact with the environment to sense their presence.**

***Keywords*- *Arduino microcontroller, auton shield, IR sensors, XBEE module, wifi camera*.**

I. INTRODUCTION

Pit avoider robot is used to avoid the pit which exiting in its path. Obstacle avoider robot is used to avoid hitting the object around the robot. It is an autonomous robot so no need for manual control. It is a logistic robot too. The sensors that present in the robot are used to have a contact with the environment. The embedded C language is used. The XBEE module is one of the main advantages of this robot. When robot gets struck at any point in its path the XBEE module is used to control the movement of the robot wirelessly. The wifi camera is used to display the path on the monitor. So, we can get clear cut information about the respective tunnel. So, the only duty of the human is to investigate the movement and the path of the robot and get the information from robot. The information is live information. Without the presence of the human the valuable information is received by using the small robot.

i. *Pit Avoider Robot*

The pit avoider robot is one of the module in this robot. This module is used to avoid the pit that present in the path of the robot. The pit is identified by using the INFRARED RED sensor. The rays that emitted from this sensor are used to find the presence of the pit.

ii. *Obstacle avoider Robot*

The obstacle avoider robot is the another module that present in this robot. This module which is used to avoid the obstacle that present at its path. Here where the same IR sensor which is used to sense the obstacle that appearance in its path.

iii. *XBEE Module*

The XBEE module which is used to control the movement of the robot over a long distance. The transmitter that fixed in the system will sends the data to the robot. The receiver is fixed in the robot and it moves according to the data.The communications taken place in range of baud rate **250 Kbit/s.** The distance for the communications is very high but it is limited. The communication which will take place up to 10 km.

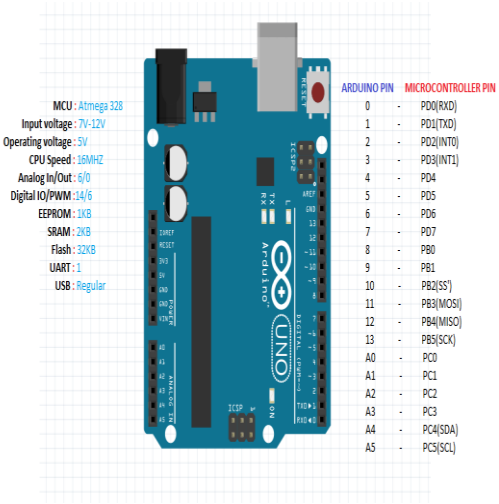
iv. *CAMERA*

The wifi camera is used here to trap the information about the path. It will give us a detail presence of the path inside the tunnel. This module which will gives you the live information about the tunnel i.e. the path of the robot.

II. ELECTRONICS COMPONENTS

There are some electronics components which is placed in this robot. Each components are important to built this robot. Their features and their importance are explained below.

ARDUINO BOARD



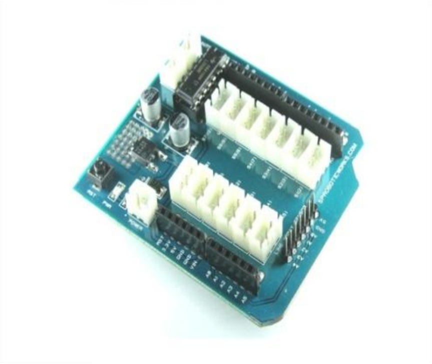
MCU : Atmega 328
Input voltage : 7V-12V
Operating voltage : 5V
CPU Speed : 16MHZ
Analog In/Out : 6/0
Digital IO/PWM :14/6
EEPROM : 1KB
SRAM : 2KB
Flash : 32KB
UART : 1
USB : Regular

ARDUINO PIN		MICROCONTROLLER PIN
0	-	PD0(RXD)
1	-	PD1(TXD)
2	-	PD2(INT0)
3	-	PD3(INT1)
4	-	PD4
5	-	PD5
6	-	PD6
7	-	PD7
8	-	PB0
9	-	PB1
10	-	PB2(SS')
11	-	PB3(MOSI)
12	-	PB4(MISO)
13	-	PB5(SCK)
A0	-	PC0
A1	-	PC1
A2	-	PC2
A3	-	PC3
A4	-	PC4(SDA)
A5	-	PC5(SCL)

This arduino board which is main heart of this robot. Where the program which is implemented in this board and the robot function according to this. The whole movement of this robot is controlled by this board. The pin ATMega328 which is placed in this board which is the brain of this whole module.

a) AUTON SHEILD

This shield which is used to place all the sensors in it. Here where maximum 12 sensors can be placed. This auton shield which is connected to the arduino board.

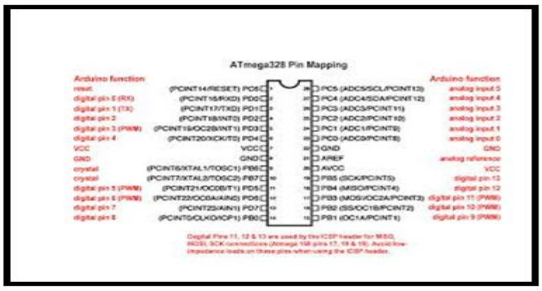


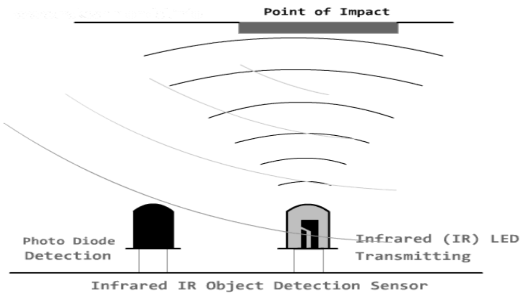
b) ATMEGA 328 PIN

This pin is the whole brain of the robot, where the program is uploaded here and it makes the robot to function according to the code that built.

c) IR SENSOR

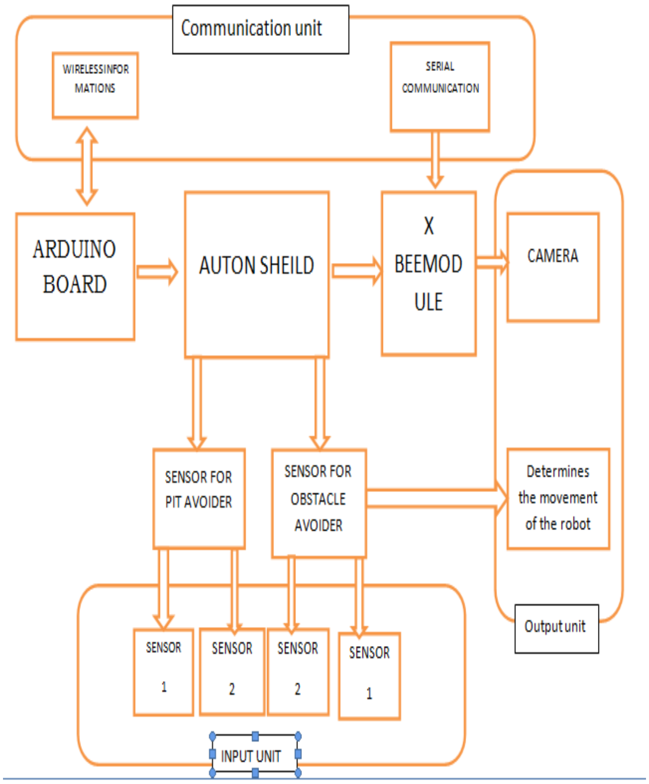
This sensor which will sense the pit and the obstacle by emitting its rays under certain frequency. The mechanism is given in diagrammatic representation below.




Point of Impact
Photo Diode Detection
Infrared (IR) LED Transmitting
Infrared IR Object Detection Sensor

III. ARCHITECTURE

The architecture of this whole robot is given in detailed diagram.



IV. METHODOLOGY

If the sensors get the input the robot will take the other path. The sensors input are the pit and the obstacle. When the sensor detects the pit it will avoid the pit and move towards another destination. The same will be applicable for obstacle avoider robot. If the robot smacked at any place XBEE module is used to control the movement of the robot wirelessly. By using the camera the live information of the current path will be gathered.

V. APPLICATION

This robot is used in analyzing the unknown and older subways and deep forest den. It gathers the information about the lair which is filled with dangers. It act as the substitute where the human cannot appear and it saves the human life.

VI. ADVANTAGES

This robot is used for the purpose of rescue mission. The movement of the robot is been controlled by the predefined program which is been imported into the microcontroller.

VII. CONCLUSION

Thus this model is used to perform various processes where the human can’t able to appear. It doesn't falls in the pit and it will not hit the objects, it follows its correct path. It gathers the information about the path without the presence of the human and the robot can be controlled wirelessly over long distance. This model is mainly used to save the human life.

REFERENCE

[1] Introduction to autonomous robot-Nikolaus Correll.
[2] Autonomous Robots - From Biological Inspiration to Implemental and Control (Intelligent Robotics & Autonomous Agents Series)- George A Bekey

FAST DATA: THE NEXT EVOLUTIONARY STEP IN BIG DATA ANALYTICS

Jetlin.C.P[#1], Anju.P[*2], Suruthivasini.S[*3]

[#1]Assistant Professor, Department of CSE, Karpaga Vinayaga College of Engineering & Technology, Chinna Kolambakkam, Maduranthagam Tk, Kanchipuram Dt. – 603308.
*[*2] III^{yr} , Department of CSE, Karpaga Vinayaga College of Engineering & Technology, Chinna Kolambakkam, Maduranthagam Tk, Kanchipuram Dt. – 603308.*
*[*3] III^{yr} , Department of CSE, Karpaga Vinayaga College of Engineering & Technology, Chinna Kolambakkam, Maduranthagam Tk, Kanchipuram Dt. – 603308.*

jetpear@gmail.com
anjuanjana795@gmail.com

***Abstract*--The big data movement was pretty much driven by the demand for scale in velocity, volume, and variety of data. Those three vectors led to the emergence of a new generation of distributed data management platforms such as Hadoop for batch processing and NoSQL databases for interactive data access. Both were inspired by their respective predecessors Google (Hadoop, BigTable) and Amazon (Dynamo DB). As we move to fast data, there's more emphasis on processing big data at speed. Getting speed without compromising on scale pushes the limits in the way most of the existing big data solutions work and drives new models and technologies for breaking the current speed boundaries.**

Keyword- Big data, fast data, Hadoop, No SQL

I. INTRODUCTION

Of the 3 "V's" of Big Data – volume, variety, velocity (we'd add "Value" as the 4th V) – velocity has been the unsung 'V.' With the spotlight on Hadoop, the popular image of Big Data is large petabyte data stores of unstructured data (which are the first two V's). While Big Data has been thought of as large stores of data at rest, it can also be about data in motion. "Fast Data" refers to processes that require lower latencies than would otherwise be possible with optimized disk-based storage. Fast Data is not a single technology, but a spectrum of approaches that process data that might or might not be stored.

It could encompass event processing, in-memory databases, or hybrid data stores that optimize cache with disk. Fast Data is nothing new, but because of the cost of memory, was traditionally restricted to a handful of extremely high-value use cases. It is often said that time is money and nowhere is this adage more pertinent than in today's digitized business world. Thanks to a host of devices and gadgets, all connected to the internet, organizations have access to data like never before.

However, this "connected" world also means that businesses face an ultra competitive globalized commercial landscape. Big Data can play a pivotal role in a business' decision-making process, but traditional database tools lack the capability to conduct ultra-fast, sub-second real-time analysis. As part of the next generation of solutions, it is time for Big Data to evolve to Fast Data.

II. BACKGROUND

Today's data scientists must analyze historical data while continuously importing new data to produce real-time results. This is what we call "Fast Data." In today's business landscape, companies need an analytics database that is specifically engineered to deliver both Big Data and Fast Data, in order to get the maximum value from the information they have.

2.1 Issues Concentrated

The same data explosion that created the urgency for Big Data is also generating demand for making the data instantly actionable. Bandwidth, commodity hardware and, of course, declining memory prices, are further forcing the issue: Fast Data is no longer limited to specialized, premium use cases for enterprises with infinite budgets. Not surprisingly, pure in-memory databases are now going mainstream: Oracle and SAP are choosing in-memory as one of the next places where they are establishing competitive stakes: SAP HANA vs. Oracle Exalytics.

Both Oracle and SAP for now are targeting analytic processing, including OLAP (by raising the size limits on OLAP cubes) and more complex, multi-stage analytic problems that traditionally would have required batch runs (such as multivariate pricing) or would not have been run at all (too complex, too much delay). Hybrid in-memory and disk have also become commonplace, especially amongst data warehousing systems (e.g., Teradata, Kognitio), and more recently among the emergent class of advanced SQL analytic platforms (e.g., Greenplum, Teradata Aster, IBM Netezza, HP Vertica, ParAccel) that employ smart caching in conjunction with a number of other bells and whistles to juice SQL performance and scaling (e.g., flatter indexes, extensive use of various data compression schemes, columnar table structures, etc.).

2.2 It's No Longer Just About Big Data, Organizations Need Fast

An analytics database is only as good or as fast as the database it rides on. Traditional database technologies were not designed to manage today's data volumes. It's no longer the norm to make queries and wait hours for the result. Delayed query results are fine if a business wants to know what happened yesterday, last week or last month, but most organizations naturally want to have real-time information for real-time decision-making. While new platforms are being created to address substantial amounts of data, many of these lack the capabilities to query and analyze data fast enough for it to be useful. Slow data can be debilitating and costly, not just monetarily but in terms of innovation.

2.3 Selecting A Next Generation Solution

Along with the speed of analyzing data, here are the key considerations that businesses should be aware of when selecting a next generation solution for Big Data analytics. Find and analyze data from multiple sources: Today's businesses typically have data stored across different platforms and infrastructures. Therefore, the Big Data analytics tool should have sophisticated interfaces that can access data across all data warehouses and be able to analyze data at its source. It also needs to be able to run on any type of platform: from standard infrastructure and single servers to dedicated server-clusters, virtualized infrastructure and public clouds.

III. THE ENTERPRISE DATA ARCHITECTURE

The enterprise data architecture is a break from the traditional siloed data application, where data is disconnected from the analytics and other applications and data. The enterprise data architecture supports fast data created in a multitude of new end points, operationalizes the use of that data in applications, and moves data to a "data lake" where services are available for the deep, long-term storage and analytics needs of the enterprise. The enterprise data architecture can be rep- resented as a data pipeline that unifies applications, analytics, and application interaction across multiple functions, products, and disciplines

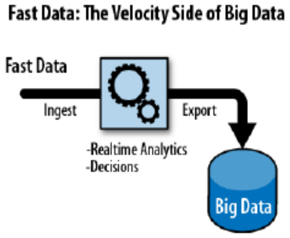


Figure 1. Fast data represents the velocity aspect of big data

3.1.1 Components Of The Enterprise Data Architecture

There is a growing recognition that volume, velocity, and variety require different models of computation and alternative processing platforms. We certainly learned this lesson in trying to deploy a Hadoop based solution for a problem. Even better, it would be desirable to build a generic data processing platform capable of handling both big data" and fast data".

The first thing to notice is the tight coupling of fast and big , although they are separate systems; they have to be, at least at scale. The database system designed to work with millions of event decisions per second is wholly different from the system designed to hold petabytes of data and generate extensive historical reports.

The architectural requirements of the separation of fast and big are evident, with the capabilities and requirements of each presented is shown below

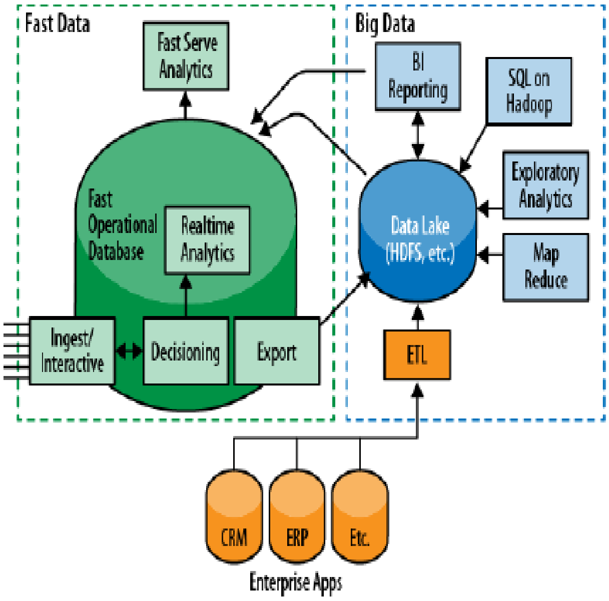


Figure 2 Note the tight coupling of fast and big, which must be separate systems at scale.

IV. BIG DATA- A DATA LAKE

The big data portion of the architecture is centered around a data lake, the storage location in which the enterprise dumps *all* of its data. This component is a critical attribute for a data pipeline that must capture all information. The data lake is not necessarily unique because of its design or functionality; rather, its importance comes from the fact that it can present an enormously cost-effective system to store everything. Essentially, it is a distributed file system on cheap commodity hardware.

Today, the Hadoop Distributed File System (HDFS) looks like a suitable alternative for this data lake, but it is by no means the only answer. There might be multiple winning technologies that provide solutions to the need. The big data platform's core requirements are to store historical data that will be sent or shared with other data management products, and also to support frameworks for executing jobs directly against the data in the data lake. In a clockwise direction around the outside of the data lake are the complementary pieces of technology that enable businesses to gain insight and value from data stored in the data lake:

Business intelligence (BI) – reporting

Data warehouses do an excellent job of reporting and will continue to offer this capability. Some data will be exported to those systems and temporarily stored there, while other data will be accessed directly from the data lake in a hybrid fashion. These data warehouse systems were specifically designed to run complex report analytics, and do this well.

SQL on Hadoop

Much innovation is happening in this space. The goal of many of these products is to displace the data warehouse. Advances have been made with the likes of Hawq and Impala. Nevertheless, these systems have a long way to go to get near the speed and efficiency of data warehouses, especially those with columnar designs. SQL on- Hadoop systems exist for a couple of important reasons:

a. SQL is still the best way to query data
b. Processing can occur without moving big chunks of data around

Exploratory analytics

This is the realm of the data scientist. These tools offer the ability to "find" things in data: patterns, obscure relationships, statistical rules, etc. Mahout and R are popular tools in this category.

Job scheduling

This is a loosely named group of job scheduling and management tasks that often occur in Hadoop. Many Hadoop use cases today involve pre-processing or cleaning data prior to the use of the analytics tools described above. These tools and interfaces allow that to happen. The big data side of the enterprise data architecture has, to date, gained the lion's share of attention. Few would debate the fact that Hadoop has sparked the imagination of what's possible when data is fully utilized. However, the reality of how this data will be leveraged is still largely unknown.

V. FASTDATA IN THE ENTERPRISE DATA ARCHITECTURE

The enterprise data architecture is split into two main capabilities, loosely coupled in bidirectional communications— *fast* data and *big* data. The fast data segment of the enterprise data architecture includes a fast in-memory database component. This segment of the enterprise data architecture has a number of critical requirements, which include the ability to ingest and interact with the data feed(s), make decisions on each event in the feed(s), and apply realtime analytics to provide visibility into fast streams of incoming data.

The following use case and characteristic observations will set a common understanding for defining the requirements and design of the enterprise data architecture. The first is the fast data capability. Data is also valuable when it is counted, aggregated, trended, and so forth—i.e., realtime analytics. There are two ways in which data is analyzed in real time:

1. A human wants to see a realtime representation of the mine, via a dashboard—e.g., how many sensors are active, how many are outside of

their zone, what is the utilization efficiency, etc.

2. Realtime analytics are used in the automated decision-making process. For example, if a reading from a sensor on a human shows low oxygen for an instant, it is possible the sensor had an anomalous reading. But if the system detects a rapid drop in ambient oxygen over the past five minutes for six workers in the same area, it's likely an emergency requiring immediate attention.

Make Faster Decisions; Don't Settle Only for Faster Analytics In order to understand the change coming to the fast data side of the enterprise data architecture, one only needs to ask: "Why do organizations perform analytics in the first place?" The answer is simple.Businesses seek to make better decisions, such as:

- Better insight
- Better personalization
- Better fraud detection
- Better customer engagement
- Better freemium conversion
- Better game play interaction
- Better alerting and interaction

5.1 Getting There: Making The Right Fast Data Technology Choices

Architectural Approaches to Delivering Fast Data. Three technology categories can be evaluated as the core components for the fast data portion of the enterprise data architecture: fast OLAP systems, stream processing products, and fast operational database systems.

Fast OLAP Systems

New in-memory OLAP systems are able to drastically reduce reporting times and enable near realtime analysis of fast-arriving data. Many of these systems are column stores, optimized for ses where the only requirement is to improve reporting speeds.

Stream Processing Systems

Stream processing has been around for decades and has proven valuable in some very specialized uses in specific industries such as capital markets trading, where very specific patterns and timings need to be identified. When used in these environments, it is a well-suited system. Stream processing systems provide scalable message processing and coordination between systems that often scales across commodity servers.

Operational Database Systems

Operational database systems are, by definition, designed to support per-event decision-making that is informed by other data stored within the system. Operational databases have long been the standard for interactive applications, but historically were unable to meet the performance required of fast data use cases.

VI. CONCLUSION

Understanding the promise and value of fast data is ernan absolute necessity, but it is not sufficient to guarantee success for companies still working to implement big data initiatives. Having the tools, and the skills, to take advantage of fast data is critical for businesses in all industries and geographies. Fast data is the payoff for big data. While much can be accomplished by mining data to derive insights that enable a business to grow and change, looking into the past provides only hints about the future. Simply collecting vast amounts of data for exploration and analysis will not prepare a business to act in real time, as data flows into the organization from millions of endpoints: sensors, mobile devices, connected systems, and the Intet of Things.

REFERENCES

[1] C. Aggarwal. Data Streams: Models and Algorithms, Kluwer Academic Publishers, Dordrecht, The Netherlands, 2007.

[2] E. Alfonseca, M. Ciaramita, and K. Hall. Gazpacho and summer rash: lexical relationships from temporal patterns of web search queries. In EMNLP , 2009.

[3] G. Ananthanarayanan, S. Kandula, A. Greenberg, I. Stoica, Y. Lu, B. Saha, and E. Harris. Reining in class of data management applications. In VLDB , 2002.

[4] R. Baraglia, F. M. Nardini, C. Castillo, R. Perego, D. Donato, and F. Silvestri. The effects of time on query ow graph-based models for query suggestion. In RIAO , 2010.

[5] D. Borthakur, J. Gray, J. S. Sarma, K. Muthukkaruppan, N. Spiegelberg, H. Kuang, K. Ranganathan, D. Molkov, A. Menon, S. Rash, R. Schmidt, and A. Aiyer. Apache Hadoop goes realtime at Facebook. In SIGMOD , 2011.

[6] M. Busch, K. Gade, B. Larson, P. Lok, S. Luckenbill, and J.Lin. Earlybird: Real-time search at Twitter. In ICDE , 2012.

[7] H. Cao, D. Jiang, J. Pei, Q. He, Z. Liao, E. Chen, and H. Li. Context-aware query suggestion by mining click-through and session data. In KDD, 2008.

"HIGHLY AUTHENTICATED" - CARDLESS ATM BANKING

T.Shunmathi [#1] and D.Swathi [*2]

#Panimalar Engineering College
*Panimalar Engineering College

Abstract **-In recent days different access control methods have been proposed to secure the ATM transaction from unauthorized access. This paper describes a method of implementing two way authentication. The first one is normal PIN verification method followed by second step of verification.In that if the authorized person replied YES through their mobile,then corresponding transaction takes place. Otherwise it switches ON the buzzer,automatically close the door of ATM centre and LCD will show the detail about ATM theft to the Higher Authorities.**

Keywords -ATM, Two way authentication, Reply Message Option(RMO), SMS.

I. INTRODUCTION

The ATM was invented to solve the problem of long queue in banks and to improve the quality of banking services to customers. With the ATM, customers can access their bank accounts in order to make cash withdrawals and check their account balances. Being a machine, it important that it authenticates the user each time he/she applies for access to ATM Services. This is usually done by the insertion of the ATM card which contains a unique card number and security information such as a PIN number which is unique to every user. Anybody can be in the possession of the card and the person mayhave knowledge of the users PIN. This makes this approach vulnerable to ATM fraud.

The two way authentication are many in use for cash withdrawal in ATM. Some of the two authentications are using mobile phones as medium to involve second step for authentication. By using mobile, a One Time Password(OTP) or One Off Transaction Password (OOTP).Or Mobile Phone Authentication Approval is the second step authentication.

II. LITERATURE REVIEW

S.T.Bhosale, Dr.B.S.Sawant(2012) has proposed the idea of Biometric scan technologies which includes finger-scan, facial-scan etc. to improve security over ATM machines. M.R.Dinesh Kumar, et.al. (2013) have proposed about two way authentication through mobiles. Navneet Sharma, Vijay Singh Rathore(2012) have achieved the goal of dual verification system using biometric technology for security.The biometric technology includes Iris, pattern, finger pattern. U.kalaiselvi et.el. (2012) proposed the system for speech recognition in ATM machines which provides security based access. M.Ajay Kumar, N. BharathKumar (2013) have proposed the system that provides the authorization at the door step itself, that is it opens door only if the card is valid.

III. EXISTING METHODOLOGY

The existing system of two-factor authentication using mobile phones, are used to generate the one time password(OTP). By definition, authentication is the use of one or more mechanisms in order to prove that you are who you can be. What you know(passwords), what you have (tokens, cards) and what you are(biometrics). Recent work has been done in trying alternative factors, for example somebody you know, a factor that can be applied in social networking.

Two-factor authentication is a mechanism that implements two of the above mentioned factors and is considered stronger and more secure than the traditionally implemented one factor authentication system. For example, withdrawing money from an ATM machine uses two factor authentication: the ATM card and the personal identification number. Passwords are known to be one of the easiest targets of hackers. Therefore, most companies are searching more ways to protect their customers and employees. Biometrics is known to very securing, but is used only in special organizations given the expensive hardware needed and their high maintenance costs. As an alternative, banks and companies are using tokens as a way of two-factor authentication.

A token is a physical device that generates passwords needed in an authentication process. Token can either be software or hardware. Hardware tokens are small devices that can be easily carried. Some of these tokens store cryptographic keys or biometric data. Anytime a user wants to authenticate in a service, he uses the one time password displayed on the token in addition to his normal account password. Software tokens are programs that run on computer and provide a onetime password that it is changed after a short amount of time. OTP algorithm's security is very important because no one should be able to guess the next password in sequence. The sequence should be random to the maximum possible extent, unpredictable and irreversible. Factors that can be used in OTP generation include names, time, seeds, etc. Several commercial two-factor authentication systems exist today such as RSA Secure ID. Multifactor authentication uses more than two form of authentication and it provides higher security.

IV. PROPOSED METHODOLOGY

This paper discusses about how the ATM transactions can be carried out through single phone call and one time password generation. The customer who wishes to withdraw money from ATM can call the toll-free number of that particular bank. Then he/she can select language for effective interaction by pressing the numbers based on the instructions specified. Then they can proceed by typing the ATM machines ID. In turn bank will authenticate the phone number and finds the corresponding PIN. It generate the dynamic code for that particular PIN at that particular time.

It sends a message containing branch_name, system_id, and then the dynamic code (i.e., One time password) generated to that phone, and also sends the same dynamic code and the PIN to the ATM machine. So the customer first selects the option of withdrawal from the displayed menu, and type the PIN and dynamic code which they received. The ATM machine verifies whether the data entered matches the data sent by the bank server. If it matches then it dispense cash. The dynamic code should be generated in the form that is never guessed by any one using some special algorithms. The project is under development.

V. RESULT

Thus this method can overcome the problem of security breach (theft) and also helps in the case of lost cards.

A SURVEY ON VIDEO SEGMENTATION TECHNIQUES

C. Bharathi [#1], R. Rajeswari [*2] and A .Sukanya[*3]

[#1] *M.Phil Research Scholar, Department Of Computer Applications, Bharathiar University, Coimbatore*
[*2] *Assistant Professor, Department of Computer Applications, Bharathiar University, Coimbatore, TamilNadu*
[*3] *Research Scholar, Department Of Computer Applications, Bharathiar University, Coimbatore, TamilNadu*

Abstract **-Video segmentation is a recent and interesting issue in the image research field, due to the enormous amount of video information available in the recent years. The objective of this survey is explaining the techniques in efficient video segmentation. An overview of various algorithms available in the literature for video segmentation, their categories and their benefits are explained.**

Index Terms- **Video Segmentation, various Techniques, Various Categories, and steps.**

I. INTRODUCTION

Segmentation can be defined as the process of partitioning data into groups of potential subsets that have same characteristics [17]. Video segmentation is a way of dividing a movie or sequence of image frames into meaningful segments [3]. Video segmentation is essential and basis for many video applications such as video cut and paste, video compression, human computer interaction, and video understanding, [12]. Applications of video segmentation are: (1) Using scene analysis, (2) Using RGB-D dataset, (3) Radiometric calibration, (4) Monocular Depth ,(5) Extraction of occlusion layers[17]. The main difference between video and image

Segmentation lies in 3-dimentional nature of video compared to 2-dimentional images[3]. The basic requirement of video segmentation and indexing is to partition a video into shots[7]. A shot is an unbroken sequence of frames and also a basic meaningful unit in a video. It represents a continuous action or a single camera operation[4]. Video segmentation has become one of the core areas in visual signal processing research. The objective of Video Segmentation and its applications is to present the latest advances in video segmentation and analysis techniques while covering the theoretical approaches, real applications and methods being developed in the computer vision and video analysis community[17].

Video segmentation generalizes the grouping of pixels sptio temp

n. The video segmentation problem is complex and has many challenges such as: (1) Temporal coherence, (2) Automatic processing and (3)Scalability.[19]

The frame work for video segmentation is depicted as shown in figure 1. Fig.1 shows the basic steps in a general video segmentation in which the video sequence is cut into scenes. Then temporal and spatial segmentation is applied. The spatially segmented output and the temporally segmented output are combined in the video sequence on the video segmentation.

Recently a low of work his being carried out in the area of video segmentation. This paper gives a brief review of various work which have been carried out in video segmentation. The rest of the paper is organized as follows. Section II describes various algorithms used for video segmentation. Section III describes the feature algorithm and section IV provides the conclusion.

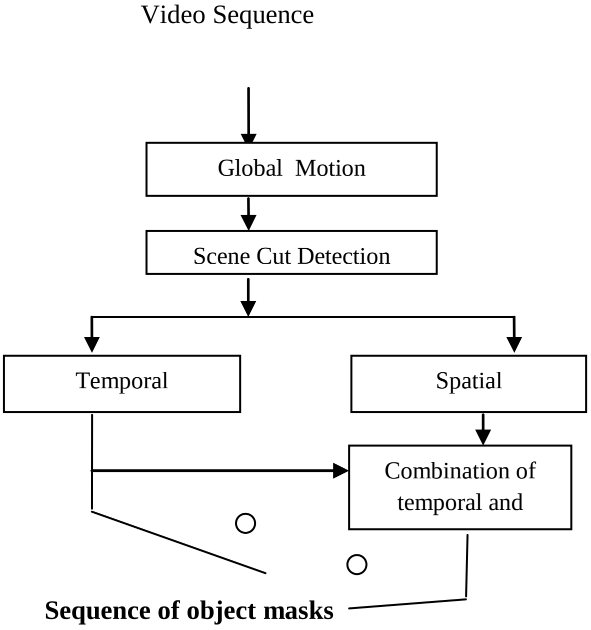


Figure1: Basic steps in video segmentation(Ref:20)

II. LITERATURE SURVEY

The various video segmentation algorithms are depicted in figure 2.

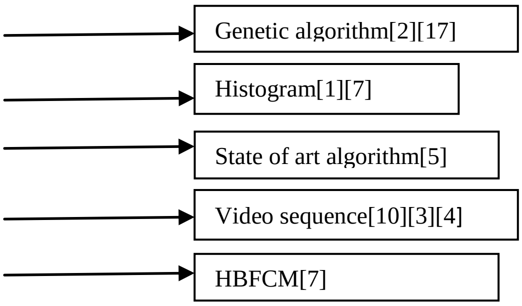


Figure 2:Various video segmentation algorithms

Kucuktunc et al [1] describes the fuzzy color histogram-based shot-boundary detection. The algorithm is specialized for content based copy detection applications. The histogram is generated in fuzzy link color and it detects the shot boundaries and false alarms to the video transformations and it is compared with state-of-the-art shot boundary detection algorithms.

Kima et al [2] proposed a novel genetic algorithm based video segmentation method. The method is based on genetic algorithm to compute the efficiency and quality of the segmentation results. The chromosomes represents frames which are classified into three groups via first chromosome , stable chromosome, and unstable chromosome. Here video model are used in the Markov random fields. This method improves the speed and segmentation quality and it is applied to the synthetic video sequences and natural video sequences.

Hua et al **[**3**]** describe a video object segmentation in rainy situations based on different scheme with object structure and color analysis. This method combines the background construction based video object segmentation and the background extraction based video object segmentation where pixel in both the foreground and background from the video segmentation are separated using histogram based edge detection method. Here histogram based method is used to detect the moving object. The shadow regions and color reflection regions on the wet ground are removed from the initial moving object masks via a diamond window mask and color analysis of the moving object. The boundary of the moving object is refined using connected component labeling and morphological operations.

Soochahn et al [4] proposed a branch-and-mincut algorithm for segmentation of video. This algorithm is used for adjacency of the key frame and it estimates what is optimal among a set of shapes in the current image. Here video segmentation utilizes high-level cues and low level cues.

Minetto et al [5] proposed the video segmentation method based on IFT (Image Foresting Transform) race algorithm. The algorithm makes minimal assumptions about the nature of the tracked object and it consists of a few connected regions, and has a well defined border. The objects to be tracked are interactively segmented in the first frame of the video, and a set of markers are then automatically selected in the interior and immediate surroundings of the object. These markers are then located in the next frame by a combination of KLT feature finding and motion extrapolation. Here the object boundaries are identified using the Image Foresting Transform(IFT). Experimental tests on real video show that the IFT is better than graph cut methods and IFTrace is robust than other state of the art algorithms.

Hung et al [6] demonstrates the probability density function(pdf) of color components of image frame. Two Hill climbing schemes use two dimensional pdf and one dimensional pdf for clustering. The clusters are merged into four color classes. Small regions are fused into adjacent large regions to obtain segmentation result. This method effectively segments the playfield regions of various sports videos.

Lo et al [7] presented the video segmentation using histogram-based fuzzy c-means clustering algorithm(HBFCM). This video segmentation method segments the video sequence into shot , where each shot represents the sequence of the frame. The HBFCM clustering algorithm is composed of three phases which are feature extraction phase , clustering phase, and key –frame selection phase. In feature extraction phase differences between the color histogram are extracted as features. Clustering phase uses the fuzzy c-means (FCM). Here group of features are grouped into three clusters which are, shot change(SC) cluster, suspected shot change(SSC) and the no shot change(NSC). The shot change frames are identified from the SC and SSC. Here the video sequences are segmented into shots and the key frames are selected from each shot. The HBFCM clustering algorithm is robust and applicable to various types of video sequences.

Zhang et al **[**8**]** proposed the multi view video based multiple objects segmentation using graph cut and spatio temporal projections. Here an automatic algorithm is used to segment multiple objects from multi view video. The Initial Interested Objects(IIOs) are extracted in the key view of the initial frame based on the saliency model. Here data pre-processing, offline operations are extracted in an unsupervised manner. Therefore the foreground/background likelihood is evaluated by fusing color, depth and occlusion cues. This algorithm shows accurate segmentation results with good efficiency and robustness.

Souza et al [9] presented the graph based hierarchical video segmentation based on a simple dissimilarity measure. Here the hierarchical video segmentation is transformed into graph partitioning problem in which each part corresponds to one supervoxel of the video and here a new methodology for hierarchical video segmentation computes a hierarchy of partitions by a reweighting of the original graph using a simple dissimilarity measure in which a not too coarse segmentation is easily inferred. This method provides temporal coherence for the following methods: p-HOScale, cp-HOScale and 2cp-HOScale. Then the hierarchy inferred by these methods produces good quantitative results when applied to video segmentation.

Wang et al[10] presented the shape prior extraction and application for geodesic distance transforms in images and video segmentation. Here the segmentation algorithm achieved impressive performance in case where the quality of the likelihood images is not satisfactory, or where multiple similar objects are in close proximity to one another. Then the shape prior knowledge in an image segmentation algorithm based on geodesic distance transform is used. The geodesic distance transform morphology operators consist of three factors which are: the geometric distance, weighted gradients and the distance to the boundary of effective shape priors extraction method that compute shape priors automatically.

Tang et al [11] presented a new foreground prediction algorithm which is called opacity propagation and it can propagate the opacity values of the former frame to the current frame by minimizing a cost function. Optical flow and probability density estimation based on a local color model are used to find the corresponding pixels of two adjacent frames. The OPSIC(opacity propagation with sudden illumination changes) algorithm is also proposed which adds a simple color transformation model and the opacity map(OM) generated by the opacity propagation algorithm is usually more accurate than the before used probability map(pm).

Guo et al [12] proposed a video human segmentation based on multiple cue integration. Video segmentation refers to the differentiation and segmentation of foreground objects from the background environment in video streams. This model describes the local color distribution in an image via training competing 1SVMs and computes the shape prior of video human objects by optical flow based motion estimation. This model improves the automatic segmentation accuracy for the subsequent frames and current frame.

Wang et al [13] proposed the Fast image and video segmentation using single-touch interaction with touch cut. It is a robust and efficient algorithm for segmenting image and video sequences with minimal user interaction. This algorithm requires only a single finger touch to identify the object image or first frame of video. This method is based on the appearance of the model fusing edge, region texture and geometric information sampled local to the touched point. The video segmentation uses the temporal coherence by incorporating motion estimation and a shape prior learned from the previous frames. Here the visual object cut-out provides a practical solution for image and video segmentation on compact touch screen devices, facilitating spatially localized media manipulation.

Ling et al [14] presented a background modeling and foreground segmentation approach based on the feedback of moving objects in traffic surveillance systems. Here a frame image is divided into four kinds of regions. Then a dual layer background updating is done for these different regions with appropriate operations to improve the quality of the background model. The predicted object blocks are merged into regions among which adaptive segmentation thresholds are used for foreground segmentation based on the spatial relationship. Here the adaptive threshold approach efficiently avoids erroneous holes and splitting in foreground segmentation and this approach is tested with several public data sets.

Xu et al [15] presented a video object segmentation and 3D trajectory estimation for monocular video sequences. This method is based on the color and motion information among video frames, therefore segments the scene, calibrates the camera, and calculates the 3D trajectories of moving objects. In this method, reliable 2D feature motions are used by comparing SIFT(Scale invariant feature transform) descriptors among successive frames and images over segmentation.

ALGORITHM	PURPOSE	MERITS
Branch and Min-cut[4]	The key frames are obtained from the Global shape foreground	The performance of the foreground object and changing topology are limited to shape .
Genetic algorithm [GAs] [2]	GAs are effective in the case of combinatorial problems as they enable parallel exploration of search space.	The method not only reduces the computational time and it produces sufficiently good quality segmentation results.
Distributed genetic algorithm [DGAs][18]	Segmentation is performed based on chromosomes that is independent and initialized using random values.	The small sized population reduces the computational time and a large sized population provide the search space.
shot-boundary detection algorithm[1]	Detects shot boundaries and reduces the false alarms	Discriminate, easy to compute, and mostly used in video frame shot detection.
IFTrace [5]	Reliably tracks the deformable objects.	Faster and more precise
Hill climbing [6]	Detect the local 2D pdf and one dimensional pdf.	The methods are effective in various video types with better performance of the segmentation accuracy and computational efficiency.
HBFCM [7]	Selects the key frame for each shot into the indexing. It does not need the threshold required for shot change detection approach. It uses SSC cluster which is not considered in the clustering approach.	Robust and applicable to various types of video sequences.
Opacity Propagation[11]	Former frame and current frame propagate the opacity value.	Computationally efficient and more accurate for the color density estimation.

III. CONCLUSION

This paper summarizes the Image Retrieval used in medical application. A short description about the Content Based Image Retrieval (CBIR) in biomedical images is given. Then about the image filter and image indexing used for retrieving images in the CBIR. The paper also describes about the features such as texture, color and shape which are used in CBIR.

COMPARATIVE STUDY ON WI-FI AND WI-MAX

K.DINESH KUMAR,[#1]

[#1]*Bachelor of Enginering in Computer Science and Engineering*, *RMK COLLEGE OF ENGINEERING AND TECHNOLOGY*

***Abstract*--We live in the era of modernization. In this 21st century, the modern civilization is hugely depended upon electronics and communication. Human seeks interaction with others not in face-to-face communication but with the help of mobility. Mobility gave birth to the wireless system of network and thrown the wire line system. In the era of 1990, we use the mobility for communication system. But now, we are ready to use the latest technologies and also the technology beyond the imagination and thinking. The Wi-Fi is the first symptom of Wireless Networking. In this paper, we are about to discuss the Architecture and working of the Wireless-Fidelity and also insist to use the better technology or a replacement for overcoming the disadvantages and drawbacks of Wi-Fi tradeoffs in varios dimensions. One simple way to categorize the different technologies is by the data rates they provide and how far apart communicating nodes can be. There are three prominent wireless technologies. They are Wi-Fi, Bluetooth and Three-generation (or) 3G cellular wireless standards.**

I. INTRODUCTION

A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. A method by which homes, telecommunications networks and enterprise installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations is known as wireless networking. Wireless telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical level of the Open Systems Interconnection model (OSI Model) network structure. Wireless Technologies differ from wired links in some important ways. here is a baffling assortment of different wireless technologies, each of which makes different tradeoffs in varios dimensions. One simple way to categorize the different technologies is by the data rates they provide and how far apart communicating nodes can be. There are three prominent wireless technologies. They are Wi-Fi, Bluetooth and Three-generation (or) 3G cellular wireless standards.

II. BACKGROUND:

Wireless does not mean sparks, noise, or a lot of switches. Wireless means communication without the use of wires other than the antenna, the ether, and ground taking the place of wires. Radio means exactly the same thing: it is the same process. Communications by wireless waves may consist of an SOS or other Messages from a ship at sea or the communication may be simply the reception of today's top 10 music artists, or connecting to the Internet to check your email. It does not become something different in either spelling or meaning. In 1971, ALOHA net seminal packet radio system that connected Hawaii Island with the radio networks was invented.2G Cellular Network was introduced in the year of 1991.Wi-Fi protocol was first released by Wi-Fi Alliance in the year of 1997.

III. EXISTING SYSTEM

Most readers will have used a Wireless Networking system based on IEEE 802.11 standards, which are referred to as Wi-Fi. Wireless Fidelity (or) Wi-Fi is technically a trademark, owned by a trade group called the Wi-Fi Alliance, which certifies the product compliance with 802.11. Wi-Fi is designed for the limited geographical area i.e., homes, office buildings, campuses etc,.Its primary challenge is to mediate access to a shared communication medium. The wireless nature of such networks allows users to access network resources from nearly any convenient location within their primary networking environment. With the emergence of public wireless networks, users can access the internet even outside their normal work environment. Wireless networking hardware is at worst a modest increase from wired counterparts. This potentially increased cost is almost always more than outweighed by the savings in cost and labor associated to running physical cables.

IV. ARCHITECTURE

Wi-Fi Architecture is a technique of designing and arrangement of different components in Wireless Local Area Networking device in a specific way. The special type of device which is the combination of transmitter and receiver known as Transceiver which is an essential part for standard Wireless LAN architecture.

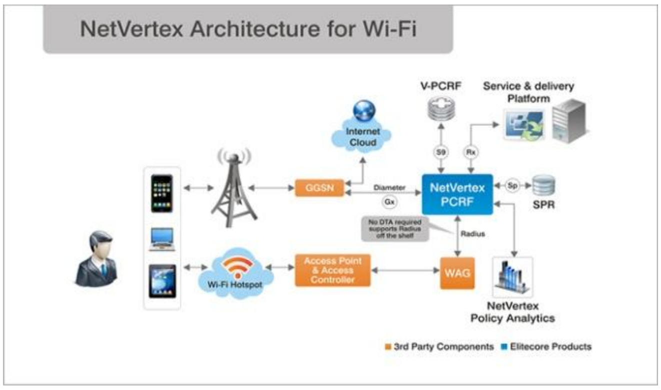

NetVertex Architecture for Wi-Fi
V-PCRF
Service & delivery Platform
Internet Cloud
S9
Rx
GGSN
Diameter
Gx
NetVertex PCRF
Sp
SPR
No DTA required supports Radius off the shelf
Radius
Wi-Fi Hotspot
Access Point & Access Controller
WAG
NetVertex Policy Analytics
■ 3rd Party Components ■ Elitecore Products

Fig.3.1.1.Wi-Fi Architecture 1.Access point 2.Clients 3.Bridge.

A The components of Wi-Fi architecture are special type of routing device that is used to transmit the data between wired and wireless networking device is called as AP. It is often connected with the help of wired devices such as Ethernet. It only transmits or transfers the data between wireless LAN and wired network by using infra structure mode of network. One access point can only support a small group of networks and works more efficiently.

It is operated less than hundred feet. It is denoted by AP. Any kind of device such as personal computers, Note books, or any kind of mobile devices which are inter linked with wireless network area referred as a client of wireless LAN architecture. A special type of connectors which is used to establish connections between wired network devices such as Ethernet and different wireless networks such as wireless LAN. It is called as bridge. It acts as a point of control in wireless LAN architecture.

DISADVANTAGES:

SECURITY

To combat this consideration, wireless networks may choose to utilize some of the various encryption technologies available. Some of the more commonly utilized encryption methods, however, are known to have weaknesses that a dedicated adversary can compromise.

RELIABILITY:

Like any radio frequency transmission, wireless networking signals are subject to a wide variety of interference, as well as complex propagation effects that are beyond the control of the network administrator.

Reliability
/re-ly-a-bi-li-ti/
1. To be able to produce good res
time after time. 2. How much a
person can be depended on.

3.2.3. SPEED: The speed on most wireless networks (typically 1-54 Mbps) is far slower than even the slowest common wired networks (100Mbps up to several Gbps). However, in specialized environments, the throughput of a wired network might be necessary.

V. PROPOSED TECHNOLOGY

WI-MAX:

After the past three decades after invention of Wireless system, we were unable to send data without any wire at high speed. In 1999, the invention of Wi-Fi revaluated the telecom industry. The latest version of Wi-Fi 2004.802.16d, started to update the Wi-Fi system. Wi-MAX (Worldwide Interoperability for Microwave Access) is a wireless communications standard designed to provide 30 to 40 megabit-per-second data rates with the 2011 update providing up to 1 Gbit/s for fixed stations. The name “I-MAX" was created by the WiMAX Forum, which was formed in June 2001 to promote conformity and interoperability of the standard.

The forum describes Wi-MAX as "a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL. Wi-MAX refers to interoperable implementations of the IEEE 802.16 family of wireless-networks standards ratified by the Wi-MAX Forum. (Similarly, Wi-Fi refers to interoperable implementations of the IEEE 802.11 Wireless LAN standards certified by the Wi-Fi Alliance.) Wi-MAX Forum certification allows vendors to sell fixed or mobile products as Wi-MAX certified, thus ensuring a level of interoperability with other certified products, as long as they fit the same profile. The original IEEE 802.16 standard (now called "Fixed Wi-MAX") was published in 2001. Wi-MAX adopted some of its technology from Wi-Bro, a service marketed in Korea.

Worldwide Interoperability for Microwave Access (Wi-MAX), is a wireless communications technology aiming to provide wireless data over long distances in a variety of ways as an alternative to cable and DSL, from point-to-point links to full mobile cellular type access. It is based on the IEEE 802.16

WIRELESS TECHNOLOGIES			
Parameters	Bluetooth	Wi-Fi	3G Cellular
Link length	10m	100m	Tens of kilometers
Data rate	2 Mbps	54 Mbps	Hundreds of Kbps
Wired technology analogy	USB	Ethernet	DSL

standard. The name Wi-MAX was created by the Wi-MAX Forum, which was formed in June 2001 as an industry-led, not-for-profit organization to promote conformance and interoperability of the standard. The goal of this deliverable is to provide an overview of the functionality and a description of the Wi-MAX network architecture.

We study and assess the coexistence and interoperability solutions between Wi-MAX and other wireless access networks, such as WLAN (IEEE 802.11) in Beyond 3G (B3G) networks. We also evaluate the special features of the Wi-MAX technology, such as the improved coverage in Non Line Of Sight (NLOS) environments, in order to examine the applicability of well-known localization techniques. Finally, we investigate the possibility of developing a new localization technique that exploits the characteristics of Wi-MAX technology and the underlying network infrastructure to deliver improved positioning accuracy. The rest of this report is structured as follows.

ARCHITECTURE:

The architecture of wireless communication systems is much simple than that of wired network connections. This is the reason why now people prefer wireless internet connections. WiMax network forum is responsible for guiding the guideline for WiMax architecture. There are three main components of WiMax network architecture. The first component is the mobile stations which are used as a source of network connection for end user. The second network is an access service network which is formed of more than two or three base stations. It also contains ASN gateways which build the radio access at the end. The third component is connectivity service network which is responsible for providing IP functions.

The base station provides the air interface for the mobile stations. The base stations also provide mobile management functions, triggering and tunnel establishment, radio resource management, dynamic host control protocol proxy, quality of service enforcement and multicast group management. ASN is responsible for radio resource management, encryption keys, routing to the selected network and client functionality. Connectivity service network is responsible for internet connections, corporate and public networks and many other user services.

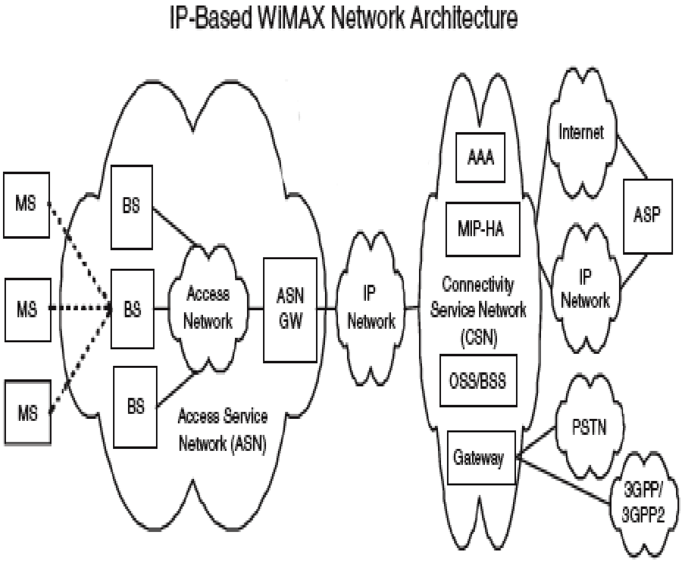


Fig.4.2.1.Wi-Max Architecture

ADVANTAGES:

The advantages of Wi-Max are as follows. Single station can serve hundreds of users. Much faster deployment of new users comparing to wired networks. Speed of 10Mbps at 10Kilometers with line-of-site. It is standardized, and same frequency equipment should work together. Wi-Max is the combination of lost cost and flexibility. WiMAX broadband networks can be quickly built at relatively low cost by installing few wireless base stations providing coverage to the surrounding area with multifunctional application: high-speed Internet, telephone service, voice and data transfer, and video applications.

Wi-Max enables high-speed voice and data transfer over long distances in remote and scarcely populated areas, as well as in densely populated areas. The wireless connectivity is not affected by the weather conditions and does not need direct line in order to work; it allows real access to end users through its own infrastructure. Wi-max products benefit service providers using their existing infrastructure investments as WiMAX has the ability to interoperate across various network types. It can leverage existing infrastructure, keeping costs down while delivering the bandwidth needed to support current system. Wi-MAX offers potential for development, new applications and opportunities.

VI. COMPARISON BETWEEN WIFI & WIMAX

Wi-MAX is exactly not a technology; it is rather than a certification mark, or 'stamp of approval‘, it is given to equipment that meets certain conformity and interoperability tests for the IEEE 802.16 families of standards. A similar confusion surrounds the term Wi-Fi, which like Wi-MAX, is a certification mark for equipment based on a different set of IEEE standards from the 802.11 working group for wireless local area Networks (WLAN). Neither Wi-MAX, nor Wi-Fi is a technology but their names have been adopted in popular usage to denote the technologies behind them. This is likely due to the difficulty of using terms like 'IEEE 802.16' in common speech and writing. Wi-MAX and Wi-Fi are both wireless broadband technologies, but they have difference in the technical execution. Wi-Fi was developed to be used for mobile computing devices, such as laptops, in LANs, but is now increasingly used for more services, including Internet and VoIP phone access, gaming, and basic connectivity of consumer electronics such as televisions and DVD players, or digital cameras. On the other hand Wi-MAX was developed as standards based technology enabling the delivery of last mile wireless broadband accesses as an alternative to cable and DSL.

features	Wi-Max	Wi-Fi
IEEE Standard	802.16	802.11
Radio Technology	Orthogonal frequency-division multiplexing	Direct sequence spectrum
BW Efficiency	<=5bps	<=0.44bps
Modulation	BPSK	QPSK
Duplex	Full	Half
Frequency Band	2-11 GHz	2.4GHz
Speed	100times faster than Wi-Fi	54-250 Mbps

Table.4.4.1.Comparison between Wi-Fi and Wi-Max

VII. CONCLUSION

Based on the comparative study on Wi-Fi and Wi-Max, Wi-Max is much far better than the Wi-Fi technology based on its advantages. The comparison shows that these features along with some other benefits that make it suitable to replace the existing wireless technologies. It removes cables that for many years ruled over the world and provides high speed data transfer rate.

Wi-Max technology has much number of applications and can be used in many places and devices such as smart phones, wireless pan networks, media access control. Although Wi-Fi is a popularly used Wireless Technology, it also has some disadvantages which is an unnoticed one. Since there is a vast

VIII. FUTURE WORK

The development of Mankind lies on the development of Technology. In future, we have to use the technology which improves the standard of living of a common man. Usage of Wi-Max should be made in large-scale. Also other Wireless technologies like Gi-Fi(Gigabyte Fidelity),Li-Fi(Light Fidelity) should also be used with some improvisation to the existing system.

REFERENCES

[1] Larry L. Peterson, Bruce S. Davie, "Computer Networking: A Systems approach", Fifth Edition, Pearson Education, 2009.

[2] James F.Kurose, Keith W.Ross,"Computer Networking-A Top-Down Approach Featuring the Internet", Fifth Edition, Pearson Education, 2009.

[3] https://en.wikipedia.org/wiki/Wirelessnetwork

[4] http://www.wifinotes.com/wlan architecture.html

[5] http://ipoint-tech.com/wireless-networking-wi-fi-advantages-and- disadvantages-to-wireless-networking/

[6] http://computer.howstuffworks.com/wimax1.htm

[7] http://www.thewonderoflight.com/wp-content/uploads /2009/01/workflow01.jpg

[8] http://www.wimaxforum.org/FAQRetrieve.aspx?ID=62687

CONTEXT – BASED ACCESS CONTROL MANAGEMENT FOR MOBILE DEVICES IN OMNIPRESENTENVIRONMENT

A.S.Meenatshi[#1], Mr. M.B.Prasanth Yokesh[#2], Mr. D. Rajini Girinath[#3], Mrs. K. Amsavalli[#4]

[#1] PG Student, Dept of Computer Science and Engineering,
[#2,#4]Assistant Professor, Dept. of Computer Science and Engineering
[#3]Professor, Dept. of Computer Science and Engineering,
Anand Institute of Higher Technology, Chennai

***Abstract*—Mobile Android applications often have access to sensitive data and resources on the user device. Misuse of this data by malicious applications may result in privacy breaches and sensitive data leakage. An example would be a malicious application surreptitiously recording a confidential business conversation. The problem arises from the fact that Android users do not have control over the application capabilities once the applications have been granted the requested privileges upon installation. In many cases, however, whether an application may get a privilege depends on the specific user context and thus we need a context-based access control mechanism by which privileges can be dynamically granted or revoked to applications based on the specific context of the user. In this paper we propose such an access control mechanism. Our implementation of context differentiates between closely located sub- areas within the same location. We have modified the Android operating system so that context-based access control restrictions can be specified and enforced. We have performed several experiments to assess the efficiency of our access control mechanism and the accuracy of context detection.**

***Index Terms*—Context-based access control, smartphone devices, security and privacy, policies, mobile applications**

I. INTRODUCTION

Wireless connectivity and the widespread diffusion of portable devices raise new challenges for ubiquitous service provisioning. Mobility of users causes frequent and unpredictable changes in user location and in consequently available resources. Access control to resources is crucial to leverage the provision of ubiquitous services and calls for novel solutions based on various context information, e.g., user location, device properties, user needs, local resource visibility. This paper presents a novel access control model that proposes the adoption of context as a first-class design principle to rule access to resources the paper proposes a context-centric access control middleware, called Unlike traditional access control, permissions are directly associated with contexts, instead of user identities/roles: any mobile user/device acquires a set of permissions by entering a specific context. We propose a context-based access control (CBAC) mechanism for Android systems that allows smart- phone users to set configuration policies over their applications' usage of device resources and services at different contexts. Through the CBAC mechanism.

II. BACKGROUND

In this section, we cover related background information on Android operating system and its access control mechanism, and some basics on location services.

2.1 Operating System and API

The Android operating systems are derived from Linux based kernels and have enhanced support for security and privacy [12]. Android is designed with a multi-layered security infrastructure, which provides developers a secure architecture to design their applications.

2.2 Permission System

The Android permission system controls which application has the privilege of accessing certain device resources and data. Application developers that need access to protected Android APIs need to s pecify the permissions they need in the AndroidManifest.xml file which ,if inaccurately assigned, can increase the risks of exposing the users'data and increase the impact of a bug or vulnerability.

Each application declares the permissions listed in its AndroidManifest.xml file at the time of installation, and users have to either grant all the requested permissions to proceed with the installation, or cancel the installation. The Android permission system does not allow users to grant or deny only some of the requested permissions, which limits the user's control of application's accessibility.

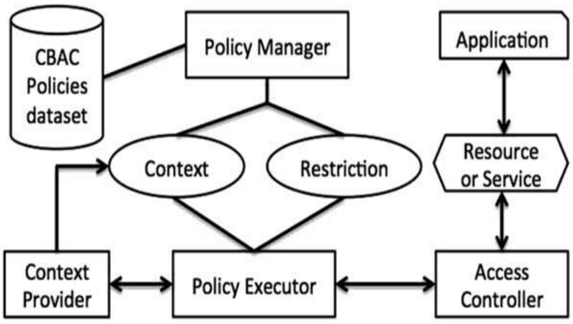
2.3 Android Application Components

Every Android application is composed of four essential Components : Activities, Services, Content Providers, and Broadcast Receivers. An Activity defines an application'suser interface. The Service component is designed to be used for background processing. The Content Provider component acts as a global instance for a particular application, so that all applications on the device can use it. It stores and manages a shared set of data belonging to the owner application using a relational database interface. Finally the Broadcast Receiver component acts as mailboxes that allows applications to register for system or application events. All registered receivers for an event will be notified by android once this event happens.

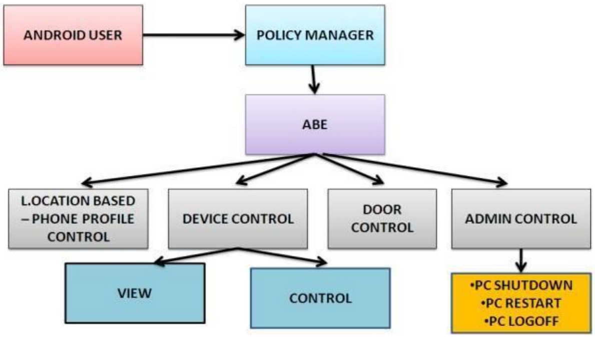
III. CELLULAR TRIANGULATION

Cellular triangulation (cell ID) is another positioning approach based on cellular technology. It refers to tracking a mobile phone'scurrt location using radio towers. Through contacting every nearby antenna tower, cellular triangulation can make a measurement of how far away the cellular mobile device is based on the signal it is transmit- ting. This is done by measuring signal strength and the round-trip signal time. Once this distance is calculated, finer approximations can be done by interpolating transmitting signals between adjacent radio towers. The accuracy of this method varies according to the density of cell towers existing in an area. For instance, the accuracy in large cities can reach up to 10 meters due to the high density of cellular towers. Our framework consists of an access control mechanism that deals with access, collection, storage, processing and usage of context information and device policies.

Fig.1 Access control Framework



IV. ARCHITECTURE DIAGRAM



Android based application is deployed and access policy is determined based on their location. If user goes to conference hall their android phone automatically goes to the silent mode. User can control / view device options inside the premises. User can control door operations while exit. Authority person can shut down, restart, logoff any client'smachine as we include ABE algorithm

5 UbiCOSM Security Framework

UbiCOSM is an access control middleware for securing service provisioning with context awareness requirements. In particular, UbiCOSM focuses on three main peculiar aspects: flexible solutions for context-centric access control, active context view provisioning to mobile users, and privacy support in the propagation of user context information. UbiCOSM access control decisions depend on dynamic context attributes, such as resource state and availability, in addition to more traditional attributes, e.g., the identity/role of user requesting a resource access.

V. UBICOSM CONTEXT MODEL

UbiCOSM access control management distinguishes two different kinds of context: physical and logical. Physical contexts identify physical spaces, delimited by specific geographical coordinates. A user operates in a particular physical context depending on her current location. At any time, one user can belong to only one physical context. Physical contexts define specific boundaries for access control policy management: each physical context holds references to the resources to be protected.

5.2 UbiCOSM Access Control Middleware

The UbiCOSM middleware services built on top of the context-aware CARMEN middleware .CARMEN provides lower-level functions for entity identification, resource discovery, directory, context management, and event registration/dispatching. On top of these services UbiCOSM furnishes the additional facilities. We herein detail the key services for the support of access control. The Context-Aware Security Manager (CASM) is responsible for computing the set of applicable context-centric access control policies for mobile clients thus establishing the active context view of any entering user. CASM calculates and return to the user a valid access context view on the basis of active context situation.

VI. CONCLUSION

In this work, we proposed a modified version of the Android OS supporting context-based access control policies. These policies restrict applications from accessing specific data and/or resources based on

the user context. The restrictions specified in a policy are automatically applied as environment UbiCOSM proposes and implements a novel context-centric access control framework specifically designed to protect resource of user personal information in ubiquitous service provisioning scenario.Our approach requires users toconfigure their own set of policies; the difficulty of setting up these configurations require the same expertise needed to inspect application permissions listed at installation time. However we plan to extend our approach to give network administrators of organizations the same capabilities once a mobile device.

REFERENCES

[1] P.Bella vista ,A.Corradi, .Montarani ,C,Stefanelli,"Dynamic Binding in Mobile Applications: a Middleware Approach",IEEE Internet Computing ,Special Issue on "Mobile Applications",Vol.7,No.2,March/April 2003.

[2] G.Neumann, M.Strembeck, "Anpproach to Engineer and Enforce Context Constraints in an RBAC Environment",ACM, SACMAT'03, Como, Italy, June 2003.

SECURITY BASED AUTOMATED SMART EB MONITORING USING LIGHT FIDELITY COMMUNICATION SYSTEM

M. Priyanka[#1], Mrs. M. Maheaswari[#2], Mr. D. Rajini Girinath[#3], Mr.N.Vasudevan[#4]

[#1] PG Student, Dept. of Computer Science and Engineering,
[#2,4] Assistant Professor, Dept. of Computer Science and Engineering,
[#3] Professor, Dept. of Computer Science and Engineering,
Anand Institute of Higher Technology Chennai

***Abstract*— Smart Meter(SM) measure energy consumption to the utility provider (UP) in almost real time, providing a much more detailed description of the consumers energy consumption compared to their analog counter parts. This increased rate of information flow to the utility provider, together with its many potential benefits, raise important concern regarding user privacy. Another concern is the cost and time to transfer the information from the smart meter to the utility provider. This paper investigates about how information is transmitted from the smart meter to the utility provider in a fast and an effective manner at low cost. The objective of this paper is to design a privacy based smart meter to measure each device energy transmit those details to the utility provider through a technology called Light Fidelity communication system.**

***Keyword*- smart meter; utility provider; light fidelity communication system; automatic meter reading;**

I. INTRODUCTION

With the adoption of smart meters (SMs) in energy distribution networks the utility providers (UPs) are able to monitor the grid more closely, and predict the changes in the demand more accurately. This, in turn, allows the UPs to increase the efficiency and the reliability of the grid by dynamically adjusting the energy generation and distribution, as well as the prices, thereby, also influencing the user demands. SMs also benefit the users by allowing them to monitor their own energy consumption profile in almost real time. Consumers can use this information to cut unnecessary consumption, or to reduce the cost by dynamically shifting consumption based on the prices dynamically set by the UPs.

SM deployment is spreading rapidly worldwide in Europe, the adoption of SMs has been mandated by a directive of the European Parliament, which requires 80% SM adoption in all European households by 2020 and 100% by 2022. However, the massive deployment of smart meters at homes has also raised serious concerns regarding user privacy. High resolution SM readings can allow anyone who has access to this data to infer valuable private information regarding user behaviour, including the type of electrical equipments used, the time, frequency and duration of usage, and even the TV channel that is being watched, as reported in. The

privacy of smart meter data is more critical for businesses, such as data centres, factories, etc., whose energy consumption behaviour can reveal important information about their business to competitors. Several methods have been proposed in the literature to provide privacy to SM users while keeping the benefits of SMs for control and monitoring of the grid. In user anonymization is proposed by the participation of a trusted third party. Bohli et al. propose sending the aggregated energy consumption of a group of users and to protect their privacy by adding random noise to their SM readings before being forwarded to the UP. Over the years, the need for electricity has grown in rapid proportions. Electric meters are devices responsible for determining these billing charges, usually on a monthly basis
and are computed in kilowatt-hours (kWh). From manual meters employing electromechanical principles, technological advancement had prompted the advent of automatic meter reading systems. Automatic meter reading (AMR) is the
technology of automatically collecting data from energy metering and the transfer of the collected data for billing and analysis. The primary driver for the automation of meter reading is not to reduce labor costs, but to obtain data difficult to obtain. AM Rs are not only used to measure power consumption, it can also be used to read water consumption, like in New York City where low-power radio transmitters installed on household water meters which send readings to a central server for billing to up to four times a day.

The AMR system to be designed and simulated in this study is intended to overcome problems in accuracy of meter reading information and to usher in wireless systems automation in the
Philippines. To achieve these, Li-Fi technology will be integrated in a Raspberry Pi single-board computer (S8C). The

security features and data transmission capabilities of Li-Fi combined with Raspberry Pi's size and programmability are some pointers considered in hypothesizing the proposed system. Moreover, the two aforementioned are yet emerging technologies since there have been minimal number of applications implemented in the country.

II. MOTIVATION

The motivation of the proposal is to achieve the following:

- low cost data transmission
- reduce manual work
- increase user's conveniences
- privacy management

III. LITERATURE SURVEY

The smart meter privacy system[1] in the presence of alternate energy source which is motivated by the information leakage and average power limitation problems they characterize the privacy-power function in a single letter from when the users' energy demands are assumed to be independent and identically distributed over time. They have shown that the optimal allocation of the energy provided by the AES in the exponentially distributed input load scenario can be derived using the reverse waterfilling algorithm. Development of secured wireless based home area network [2] for metering in smart grid which requires the active participation of consumers to improve the quality and reliability of the power delivery. Due to the shared nature of the wireless medium, however, these deployments face security challenges and interference issues which must be addressed while developing it.

The Automated Meter Reading (AMR) system[3] is more advantageous than conventional electromechanical meter reading system since electric metering system is more accurate measuring device. Electromechanical metering system puts consumers at a disadvantage as the accuracy of the power consumption is being compromised The Light Fidelity communication system[4] that makes use of LED light which helps in the transmission of data much faster and flexible than data that can be transmitted through Wi-Fi. By using visible light as transmission medium, Li-Fi provides wireless indoor communication. The bit rate achieved by Li-Fi cannot be achieved by Wi-Fi. Security would be snap, if you can't see the light, you can't access the data. Wi-Fi gives us speed up to 150 mbps as per IEEE802.11n,[5] which is not sufficient to accommodate number of desired users. But Li-Fi can produce data rates faster than 10 megabits per second, which is faster than the average broadband connection.

IV. CONCLUSION OF LITERATURE SURVEY

Automated smart EB monitoring system developed in thispaper demonstrates the measurement of energy consumption of each device individually by designing the automated smartEB monitoring system. Light Fidelity Communication system transmits the data (consumption details) in a faster and flexibleway when compared to Wi-Fi technology.

A. SMART LIGHTNING

Lamp Technology which is electrode free using Li-Fi has been created for projection display applications. An optics set is used to convert light into an output which is efficiently accepted by the projector.

B. MEDICAL AND ANALYTICAL APPLICATIONS

Earlier xenon HID light sources were used which has been redesigned using the Li-Fi light source. By using light sources in hospitals and laboratories, maintenance costs can easily be lowered down because its lifetime has been increased more than five times relative to the used previously.

C.UNDERWATER COMMUNICATION

For short distances underwater visible light can support high speed data transmission as RF doesn't work. This could enable the divers and underwater vehicles to pass voice messages to each other. In such systems, microphone is installed in the LED light. The voice from a diver will be picked up with that microphone and will be sent to other diver over the light. The second diver will receive the light, accept the audio signal from the light and send acknowledgement to the other diver.

D. TRAFFIC SIGNALS

In traffic signals, LI-FI can be used which will communicate with the LED lights of the car and number of accidents can be decreased.

REFERENCES

[1] Jesus Gomez-Vilardebo and Deniz Gunduz "Smart meter privacy for Multiple Users in the presence of alternative Energy Source" IEEE transactions on information forensics and security, vol. 10, no. 1, january 2015

[2] Surya Narayan Mohapatra, Babak Karimi, "Toward a Secure Wireless-Based Home Area Network for Metering in Smart Grids" IEEE systems journal, vol. 8, no. 2, june 2014

[3] Altir Christian D. Bonganay, JosefC. Magno, Adrian G. Marcellana, John Marvin E. Morante, Noel G. Perez,"Automated electric Meter Reading and Monitoring system using ZigBee-Integrated Raspberry Pi single Board Computer via Modbus"

[4] Network Security: Li-Fi: Data Onlight Instead of Online, Vinod Saroha, Ritu Mehta International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 1, Jan 2014 Page No. 3681-3688

SMART BANK GUARD SECURITY SYSTEM IMPLEMENTATION WITH THEFT IDENTIFICATIONUSING PATTERN ANALYZER

P. Sugapriya[#1], Mrs. K. Amsavalli[*2], Mr. K. Karnavel[$3], Ms. R. Elakiya[@4]

[#1] *PG Student, Dept. of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai*
[*]*2 Assistant Professor, Dept. of Computer Science and Engineering, Anand Institute of Higher Technology*
[#3] *Assistant Professor, Dept. of Computer Science and Engineering, Anand Institute of Higher Technology*
[@4]*Assistant Professor, Dept. of Computer Science and Engineering, Anand Institute of Higher Technology*

***Abstract* –Security and Authentication of individuals is necessary for our daily lives especially in Bank lockers. But the security provided with bank systems has some back-doors. It has been improved by using techniques like pattern recognition comparing these existing traits, there is still need for considerable computer vision. Pattern recognition is a particular type of biometric system that can be used to reliably identify a person uniquely by analyzing the patterns found in OPEN CV image processing is used in this security system to authenticate user. In this system a new approach is provided for banking system. Initially pattern flow are collected as datasets and maintained in bank agent server. The machine has a camera to capture the pattern flow of user and sent for processing features of the logic were compared and user where recognized. In addition to the authentication of user there is another system to identify the user before that RFID tad checking is needed. Image processing is used and keypad password is needed for another level of security.**

***Index Terms*– Introduction, Security, Smart Card, Authentication, Wireless Communication, Open CV, Password.**

I. INTRODUCTION

Banking is one of the sectors where technology and advancements in technologies have not been utilized to the fullest potential. Be in security system or access systems or even in material handling in banks. For example in the security systems even today very old practices are followed that can be made lot better using technologies like open CV which is easily usable and also easy to implement at a consumer level. In this present age, safety has becomes an essential issue for most of the people especially in the rural this system may not be good for all the time. In this paper we have implemented safety of the money in the bank locker, house, and office (treasury) by using RFID and GSM technology which will be more secure than other systems. Radio-frequency identification (RFID) based access-control system allows only authorized persons to open the bank locker with GSM technology. Basically, an RFID system consists of an antenna or coil, a transceiver (with decoder) and a transponder (RF tag) electronically programmed with unique information. There are many different types of RFID systems in the market. These are categorized on the basis of their frequency ranges. Some of the most commonly used RFID kits are low-frequency (30-500 kHz), mid-frequency (900 kHz-1500MHz) and high-frequency (2.4-2.5GHz)[1]. The passive tags are lighter and less expensive than the active tags. Global system for mobile communication (GSM) is a globally accepted standard. Several GSM is a common European mobile telephone standard for a mobile cellular radio system operating at 900 MHz In the current work,SIM300 GSM module is used. The SIM300 module is a Tri-band GSM/GPRS solution in a compact plug in module featuring an industry-standard interface. It delivers voice, data and fax in a small form factor with low power consumption. In this paper we have designed and implemented a bank locker security system based on RFID and GSM technology. In this system only authentic person can be recovered money from bank locker with two password protection method.

Implementing sensors vibration, temperature sensor on the door side for security purpose and on machine side three level of authentication is needed .first one is RFID tag is provided for authentication of user id ,next camera is installed to capture the pattern password of user and with the help of image processing using OPEN CV to recognize the user pattern and the authentication for banking is provided and keypad password is need another level authentication for users access of banking is permitted for thief an immediate door lock is applied and intimate message to bank manager. This system is secure and less cost it will be a best banking system. Timer is on for accessing the bank locker it's locked automatically while the user exceeds the time as well as message notification also intimated to the manager.

II. MOTIVATION

The motivation of the proposal is to achieve the following:

- More secure
- Authentication only used
- privacy management

III. LITERATURE SURVEY

1. Prabhakar and pankanti(1997) proposed Biometrics offers greater security and convenience than traditional methods of personal recognition. In some applications, biometrics can replace or supplement the existing technology.

2. Mary Lourde and Dushyant Khosla (2010) says Perhaps the most important application of accurate personal identification is securing limited access systems from malicious attacks. Among all the presently employed biometric techniques, fingerprint identification systems have received the most attention due to the long history of fingerprints and their extensive use in forensics. This paper deals with the issue of selection of an optimal algorithm for fingerprint matching in sorder to design a system that matches required specifications in performance and accuracy.

3. Gayathri and Selvakumari (2014) Access control system forms a vital link in a security chain. The Fingerprint and password based security system presented here is an access control system that allows only authorized persons to access a restricted area. We have implemented a locker security system based on fingerprint, password and GSM technology containing door locking system which can activate, authenticate and validate the user and unlock the door in real time for locker secure.

4. Arun Ross and salil prabhakar (2004) 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.

5. Kamble and Bharti (2012) the biometrics, fingerprint recognition is one of the most reliable and promising personal identification technologies. Fingerprints are the most widely used biometric feature for person identification and verification. But in this paper we proposed that fingerprint verification of ATM (Automatic Teller Machine) security system using the biometric with hybridization. The fingerprint trait is chosen, because of its availability, reliability and high accuracy.

6. Abhijeet Kaleand Sunpreet Kaur Nanda (2012) The GSM based communication helps the owner and concerned authorities to take necessary and timely action in order to prevent the theft. The LDR circuit is interfaced using a relay circuit with an Arduino microcontroller board. Efficacy of the proposed system can be seen in its immediate intimation regarding the incident. The proposed designed system is very effective and inexpensive.

IV. CONCLUSION

In this paper, we have first reviewed the recently proposed we are using locker key for banking though they are secured there are some disadvantages .It may be provide wrong person access the account. So in our project we are implementing sensors vibration, temperature sensor on the door side for security purpose and on machine side three level of authentication is needed .first one is RFID tag is provided for authentication of user id ,next camera is installed to capture the pattern password of user and with the help of image processing using OPEN CV to recognize the user pattern and the authentication for banking is provided and keypad password is need another level authentication for users access of banking is permitted for thief an immediate door lock is applied and intimate message to bank manager this system is secure and less cost it will be a best banking system. Timer is on for accessing the bank locker it's locked automatically while the user exceeds the time as well as message notification also intimated to the manager.

REFERENCES

[1] Prabhakar,s, pankanti s,and jain, A.K "Biometric recognition:Security and privacy concern:Security and Privacy,IEEE Volume:1 Issue:2.

[2] Mary Lourde R and Dushyant Khosla "Fingerprint Identification in Biometric Security Systems" International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010

[3] M.Gayathri, P.Selvakumari, R.Brindha "Fingerprint and GSM based Security System" International Journal of Engineering Sciences & Research Technology, ISSN: 2277-9655, Gayathri et al.3(4): April, 2014.

[4] Anil K. Jain, Arun Ross and salil prabhakar "An Introduction to Biometric Recognition"IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, no. 1, January 2004.

[5] D.Shekar and Goud and Ishaq Md and PJ.Saritha "Secured Approach for Authentication System using Fingerprint and Iris"

WIRELESS HUMAN MACHINE INTERFACE WITH DEDICATED SOFTWARE USING GOLDFINGER

S. Rajkumar[#1], K. Karnavel[#2] D.Anand Joseph Daniel[#3], P. Karthick[#4]

[#1]PG Student, Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai.
[#2,3,4]Assistant Professor, Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai.

***Abstract*--The Human Machine Interface (HMI) includes the machine like system and required signal and control the state of electronic signals through hands. People use their hands to interact with tools and other people every day. Almost continuously, we send messages and commands by hand, and through our hands, we perceive the world around us. Thus, it is not surprising that the most natural way to interact with machines is through the direct use of hands without intermediate peripherals, include the electronics required to detect, position or identify an object or rotating axis in the movement of fingers such as hand and leg. When personal computers (PC) were born, the only way to provide input to them was through hardware interfaces, and the only way to perceive outputs from PCs was through monitors or displays. In many cases, the situation currently remains almost the same. Similar considerations are valid for many machines, systems and implants that normally contribute to our everyday life. HMI provides a visual representation of a control system and provides real time data acquisition. An HMI can increase productivity by having a centralized control center that is extremely user-friendly. Additionally, the battery discharge time is reduced due to the power harvested from integrated piezoelectric transducers, which generate power from finger motions.**

***Index Terms*- Human-machine interface, wearable device, microcontroller, machines control, biomechanical energy harvesting, power management**

I. INTRODUCTION

GoldFinger, the HMI glove prototype model, has the potential to overcome some of these limitations to the integration of advanced materials, miniaturization of components and electronics, and power generation through biomechanical energy harvesting. Hand motions are used to communicate with the controller via a LED tracking system. Then, information is digitalized with dedicated software that also provides the machine microcontroller programming in the C language. When personal computers (PC) were born, the only way to provide input to them was through hardware interfaces, and the only way to perceive outputs from PCs was through monitors or displays. In many cases, the situation currently remains almost the same. Similar considerations are valid for many machines, systems and implants that normally contribute to our everyday life. In many interfacing actions, the user has to modify his natural behavior and his spontaneous posture to start a dialogue with a machine; a machine is like a foreign body to humans, to which people must conform to reach its full potential.

In the last 30 years, researchers developed several new types of interfaces between humans and machines, and currently, the HMI (human-machine interface) discipline is active in finding solutions to overcome these technological frontiers. Originally, the idea was to clothe the human body, in particular, the hands, with electro-mechanical devices that are able to sense motion and posture and convert them to

information that is usable for the machine. A number of glove systems were introduced, starting in the 1970s, which were designed to measure hand configuration in terms of bending and joint rotating angles.

The sensors used for this purpose were usually piezo resistive or light-based. The crucial features of any electric system is the power supply; these initially proposed sensing clothes were literally covered by cables and connectors, and even the latest versions still require an electric supply from wires or batteries. Regarding this topic, the next frontier is the integration of power generators into the system to convert body kinetic energy to electricity; for glove-based systems, the kinetic energy of the fingers can be stored and then used to supply the embedded electronic interfaces. Eventually, the same energy could also serve to actuate integrated feedback devices without using cables or heavy batteries.

In recent years, the PC was the favorite machine for use with experiment that involved new methods of communication under the software engineering push for virtual reality, computer graphics, computer animation, and so on. By contrast, the impact of wearable communication interfaces on mechanical systems, extensive machines, implants and industrial equipment is still weak and almost unexplored. The concept of a wearable interface for mechanical, medical and industrial systems is the natural evolution of remote controllers, which are presently used. This glove-based system converts the motion of the fingers to digital information through a LED optical communication system. Then, each set of coordinates corresponding to the original gesture is associated with a machine command accordingly to a codification previously decided. The dedicated software developed to manage the HMI provides a graphical interface for the user, the light tracking function and the continuous programming of the machine microcontroller, which is updated with every input command from the hands. The HMI glove is able to harvest the power generated by bending the finger joints by means of piezoelectric transducers integrated into the fabric. The electronic circuit can convert the voltage generated by the transducers into a rectified and leveled voltage. The results of performance evaluations demonstrated that the

energy provided by the harvesting system increases the battery duration, depending on the usage of the integrated light emitter.

II. MOTIVATION OF RESEARCH

The motivation of my research is to increase the generation of energy with low cost using power sensing circuit.

- Check power management using LCD.
- How much of energy is increased?
- Have low cost with high energy implemented?

III. LITERATURE SURVEY

1. T.Takahasi and F.Kishino (1991) proposed a hand gestures are one means of interaction between computers and humans. A hand gesture interface device, the VPL data glove provides real time information on a user's hand movement. Central to the proposed architecture is hand gesture interface between movements. This paper describes the movements of the hand gesture.
2. D.J.Surman and D.Zeltzer (1994) says that key hand-tracking technologies and applications using glove-based input. Hand-tracking may use various technologies such as position tracking, optical tracking, and magnetic tracking and so on. Various glove.

IV. CONCLUSION

The Gold Finger glove demonstrates the applicability of piezoelectric transducer harvesting in HMIs by reducing the power consumption with small, compact and integrated components. The HMI prototype that was fabricated showed appreciable properties, such as wireless communication, high wearability comfort, and low resistance to finger motion, and longer battery discharge times and/or smaller battery sizes because of the energy harvesting system.

Integrated piezoelectric transducers and miniaturized rectification-leveling circuitry provided a duty cycle of approximately 147.5 to the device. The Gold Finger glove demonstrates the applicability of 3-axis accelerometer harvesting in HMIs by reducing the power consumption with small, compact and integrated components. The HMI prototype that was fabricated showed appreciable properties, such as wireless communication, high wearability comfort, and low resistance to finger motion, and longer battery discharge times and/or smaller battery sizes because of the energy harvesting system. Integrated piezoelectric transducers and miniaturized rectification-leveling circuitry provided a duty cycle of approximately 147.5 to
the device.

REFERENCES

[1] T. Takahashi, F. Kishino, "Hand gesture coding based on experiments using a hand gesture interface device," SIGCHI Bull., vol. 23, no. 2, pp. 67-74, 1991.

[2] S. Bryson, C. Levit, "The virtual wind tunnel," IEEE Comput. Graph. Appl, vol. 12, no. 4, pp. 25-34, 1992.

[3] D. J. Sturman, D. Zeltzer, "A survey of glove-based input," IEEE Comput. Graph. Appl., vol. 14, no. 1, pp. 30-39, 1994.

[4] N. Karlsson, B. Karlsson, P. Wide, "A glove equipped with finger flexion sensor as a command generator used in fuzzy control system," IEEE Trans. Instrum. Meas., vol. 47, no. 5, pp. 1330-1334, 1998.

[5] J. J. LaViola, "A survey of hand posture and gesture recognition techniques and technologies," Brown Univ., Providence, RI, Tech. Rep. CS-99-11, 1999.

A STUDY ON COMPUTER-AIDED DIAGNOSIS OF ALZHEIMER

V.Punitha[#1], R.Rajeswari[*2]

[#1]*M.Phil Research Scholar, and* [#2]*Assistant professor*
[*2]*Department of Computer Applications School of Computer Science and EngineeringBharathiar UniversityCoimbatore, India*

***Abstract*--Alzheimer'sdisease(AD) is one of othe chronic neurological diseases. There are various methods available in the literature for the diagnosis of AD using computers. In this paper, the various stages of the computer aided diagnosis of AD namely; preprocessing, feature extraction, feature selection and classification are described. The paper also gives a review of the recent literature in this area. This paper presents an overview of the various stages of CAD of AD and highlights on the recent work on the detection and diagnosis of AD. The rest of this paper is organized is as follows. Section 2 describes some of the recent work in early detection and diagnosis of AD Section 3 describes the main stages of CAD of AD. Section 4 concludes the paper**

***Keywords* - Alzheimer's disease, feature extraction, feature selection**

I. INTRODUCTION

Azemr dsaeoneofth chronic neurodegenerative and age related diseases The symptoms of lhie‘sare memory loss and difficulties with thinking problem-solving or language. The disease starts mild and gets progressively worse which causes even death [2].In this disease proteins build up in te ban t om a srcue cle paus‘ ad a These structures lead to death of nerve cells and loss of brain tissue due to loss of connections between nerve cells. Detection f Azemr‘ies, stages is very useful for the early diagnosis and treatment of disease. But visual reading and semi-quantitative analysis leads to challenges in early detection of this disease. Hence there is a need for computer aided diagnosis (CAD) of medical images which will be useful to pyiin o al eeto(AD).feature intervals flhie‘s (VFI) to derive a quantitatives index of CAD systems evaluate and analyze the complex patterns related to the disease and are used to interpret the condition of the disease [3]. The various stages of CAD are preprocessing, segmentation, analysis of regions of interest and evaluation/ classification [12].

There are various software packages available for diagnosis of AD. Automated brain morphometry is used to analyze the structural changes during normal aging and progression of certain disease. Voxel-based morphometry (VBM) is a fully automated method that detects differences in the local synthetic of brain tissue on a voxel-wise comparison of multiple brain images [4]. Several image analysis software packages, such as SPM [21], FSL [25], FreeSurfur [26], ***computer***Brainvisa [27], ***aidedMindbogglediagnosis*** [28], are available which are used to process brain images. Statistical parametric mapping (SPM) is widely used in neuroscience. SPM is basically voxel based morphometry method [2]

II. RECENT WORK ON EARLY DETECTION AND DIAGNOSIS OF AD

Plant et al demonstrated three different classifiers including support vector machine (SVM), Bayes statistics, and voting pattern matching for the prediction of the conversion from mild cognitive impairment (MCI) to AD. Clustering algorithm, feature selection algorithm and classification algorithm are used to obtain a classification accuracy of up to 92%. On the clustered data linear SVM performed best with 97.62% in accuracy, VFI resulted in an accuracy of 88.1% and Bayes resulted in an accuracy of 85.71% [1]. Khedher et al have proposed computer aided diagnosis (CAD) using structural Magnetic Resonance Images (MRIs). The method performs unsupervised segmentation to obtain tissue classification of gray matter (GM),), white matter (WM) in the brain.PLS and PCA algorithm used used to generating set of AD and normal images.

Further classification is performed using SVM classifier [3] Ali et al used a combination of simplified fuzzy adaptive resonance theory map (SFAM) and Adaptive Resonance Theory Map-familiarity discrimination (ARTMAP-FD) as classifier to produce better classification performance for AD early stage detection. The Classification Accuracy rate CA) result is 95% based on single average waveform by applied method of independent component analysis (ICA)and Principal Component Analysis (PCA) [7]. Seixas et al examined diagnosis of dementia AD and MCI to implement a Bayesian Network (BN) decision model The random variables are associated with various approaches where as symptoms, signs, test result and background information‘s to Ramirez build etal proposed decisiona computer aided model diagnosis (CAD)based on probabilistic approach.

A parameter estimated using supervised learning algorithm is used to process clinical images. [8] Ortiz et al author presents Alzheimer‘s disease (AD) using structural Magnetic Resonance Images (MRIs). The method performs unsupervised segmentation to obtain tissue classification of gray matter (GM), white matter WM) in the brain. Learning vector quantization (LVQ) and SOM clustering algorithm used to generating set of AD and normal images. Further classification is performed using SVM classifier. The proposed tool yields classification result upto 90% for normal and AD patients [9] Martinez-Murcia presents a new CAD system to detect early stages of AD that consists of three stages: voxel selection, feature extraction and classification.

They have proposed a method in which voxels are selected by using Mann–Whitney–Wilcoxon U-Test. Then, factor analysis is used for feature reduction, by extracting and loading common images from the selected voxels. Finally a Linear Support Vector Machine (SVM) classifier is used to perform clustering of the input images. Two distinct databases are used in the proposed method and the achieved accuracy results are 93.7% and 92.9% for SPECT and PET images respectively [12]. Chaves et el proposed a system that consists of four stages:

(i) Preprocessing, (ii) voxel selection, (iii) feature extraction, and (iv) SVM classification. The spatial and intensity normalization is performed using activation estimation (AE) and AR mining techniques which are used to enable voxel selections. Then PCA or PLS are used to further reduce the dimension of the input feature vector and the output is given to a kernel SVM classifier. The AR FS- based method provides 91.75%, 95.12% and 89.209% in terms of accuracy, sensitivity and specificity [13]. Park et al examined classification results using 278 spectra and achieved 95.8% classification rates for MLP (multi-layer perceptron). The classification result of PCA and PLS-DA method with the full spectrum together with the feature selection methods are 84.2% and 86.0% respectively [14].

Segovia et al used Single Photon Emission Computed Tomography (SPECT) feature extraction to improve accuracy of CAD system for AD. They use a Partial Least Squares algorithm for extracting score vectors and the Out- Of-Bag error for selecting a number of scores that are used as features. Using support vector machine based classifier determines the underlying class of the images they yields accuracy rates over 90% [16] for the early emission computed tomography (SPECT) image classification. They proposed a system based on PLS, PCA feature extraction and a random forest predictor (RF).

They achieved better performance accuracy and sensitivity results [17]. Illan et al proposed a method based on automatic feature selection and combination of component-based support vector machine (SVM) for classification. The proposed approach based on the use of PCA and kernel SVM resulted in 96.91% accuracy for SPECT images [18]. Lopez et al achieved accuracy results of upto 96.7% and 89.52% for SPECT and PET images. For feature extraction technique they have used Principal component analysis (PCA) and enhanced their method using other approaches such as linear discriminant analysis (LDA) and Fisher discriminant ratio (FDR) for feature selection. The final features selected are used as inputs to neural networks (NN) and support vector machine (SVM) classifiers to accomplish computer aided diagnosis (CAD) system for automatic evaluations of neuro images presented by them [19].

Termenon et al applied relevance vector machines (RVM), nearest-neighbor (1NN) and linear support vector machines (LSVM) as classifiers for the classification of AD images. Lattice independent component analysis (LICA) across volumes is used for feature selection on fractional anisotropy (FA) data to perform classification. Feature selection is done on the between the LICA residuals at each voxel site and the data indicative variable [20]. Górriz et al

TABLE 1: summary of the methods used for diagnosis of AD

intensities directly as features (VAF) diagnosis of Alzheimer‘s dis they reduced dimensionality and featurespaceof intensity levels inside the Gaussians [21].

III. PREPROCESSING AND NORMALIZATION

Statistical parametric mapping (SPM) [15] is the most widely used software tool to analyses and evaluate brain images in research. It has been widely applied for AD and MCI and its risk groups in both cross sectional and longitudinal analysis. Current version of SPM, such as SPM99, SPM2, SPM8 and SPM5, permits anatomic standardization of SPECT or PET data either with or without MRI co registration. SPM provides less computational

3.2 Feature Extraction

Existing features are transformed into a lower dimensional space. The Well-known unsupervised feature extraction method is Principal Component Analysis (PCA) [13].

Principal component analysis (PCA) [7] [21] is the most used technique for feature reduction which means transforming the original features into a lower dimensional space. PCA, as a linear technique, is a quantitatively rigorous method for achieving data dimensionality reduction of the extracted features. PCA is used abundantly in all forms of analysis from neuroscience to computer graphics—because it is a simple, non-parametric method of extracting relevant information from confusing data sets [19].

LDA [21][19] is a generalization of Fisher's linear discriminant and is used in statistics, pattern recognition and machine learning to find a linear combination of features which characterizes or separates two or more classes of objects or events. The resulting combination may be used as a linear classifier or, more commonly, for dimensionality reduction before classification.

PLS [13][12][17] regression is a recent technique that generalizes and combines features from principal component analysis and multiple regressions. Its goal is to predict or analyze a set of dependent variables from a set of independent variables or predictors.

3.3 Feature Selection

Feature selection is the process of selecting a subset of existing features without any transformation to build robust learning models [14]. In many machine learning problem

this type of technique can improve the efficiency and accuracy. It also helps people to improve their knowledge about data by telling them which features are important and how they are related to each other.

3.4 Classification

Various classifiers have been used in the literature to classify AD from normal subjects. In this paper Support Vector Machine based classification of AD is reviewed. SVM introduced after 70s [12], is an effective supervised software tool widely used to obtain feasible solution with good generalization capability. Several studies [10] [11] have demonstrated the high performance accuracy of using

SVM to detect Alzheimer‘s[AD] . Superviseddisease learning methods are generally used in pattern recognition,voice activity detection (VAD), and classification and regression analysis. One of the main reasons for selecting SVM as classifier is to reduce number of available samples in comparison to its dimensionality [9]. SVM classifier is used to analyze medical image, classification and other application in bioinformatics.

Literature		**Data**	**Technique**		
References	**Author**		**Feature extraction**	**Feature selection**	**Classification**
1	Plant et al	MRI	Clustering algorithm		SVM Bayes VFI
2	Ramirez et al	SPECT PET	SMO	FDR	SVM
3	Khedher et al	MRI	PLS PCA		SVM
9	Ortiz et al	PET	LVQ PLS		SVM KNN
12	Martinez et al	SPECT PET	PLS	MWW	SVM
13	Chaves et al	SPECT PET	PCA PLA		SVM
14	Park et al	Raman spectroscopy	PCA PLS-DA	SFS SPA	MLP
16	Segovia et al	SPECT	PLS	FDR	SVM
17	Ramirez et al	SPECT	PLS PCA		Random Forest
18	Illan et al	SPECT	PCA ICA		Kernel-SVM
19	Lopez et al	SPECT PET	PCA	LDA FDA	SVM or NN
20	Termenon et al	MRI DTI		LICA	RVM 1NN LSVM
21	Gorriz et al	SPECT	GMM	EM	SVM

IV. VARIOUS STAGES IN COMPUTER-AIDED DIAGNOSIS OF ALZHEIMER’S DISEASE

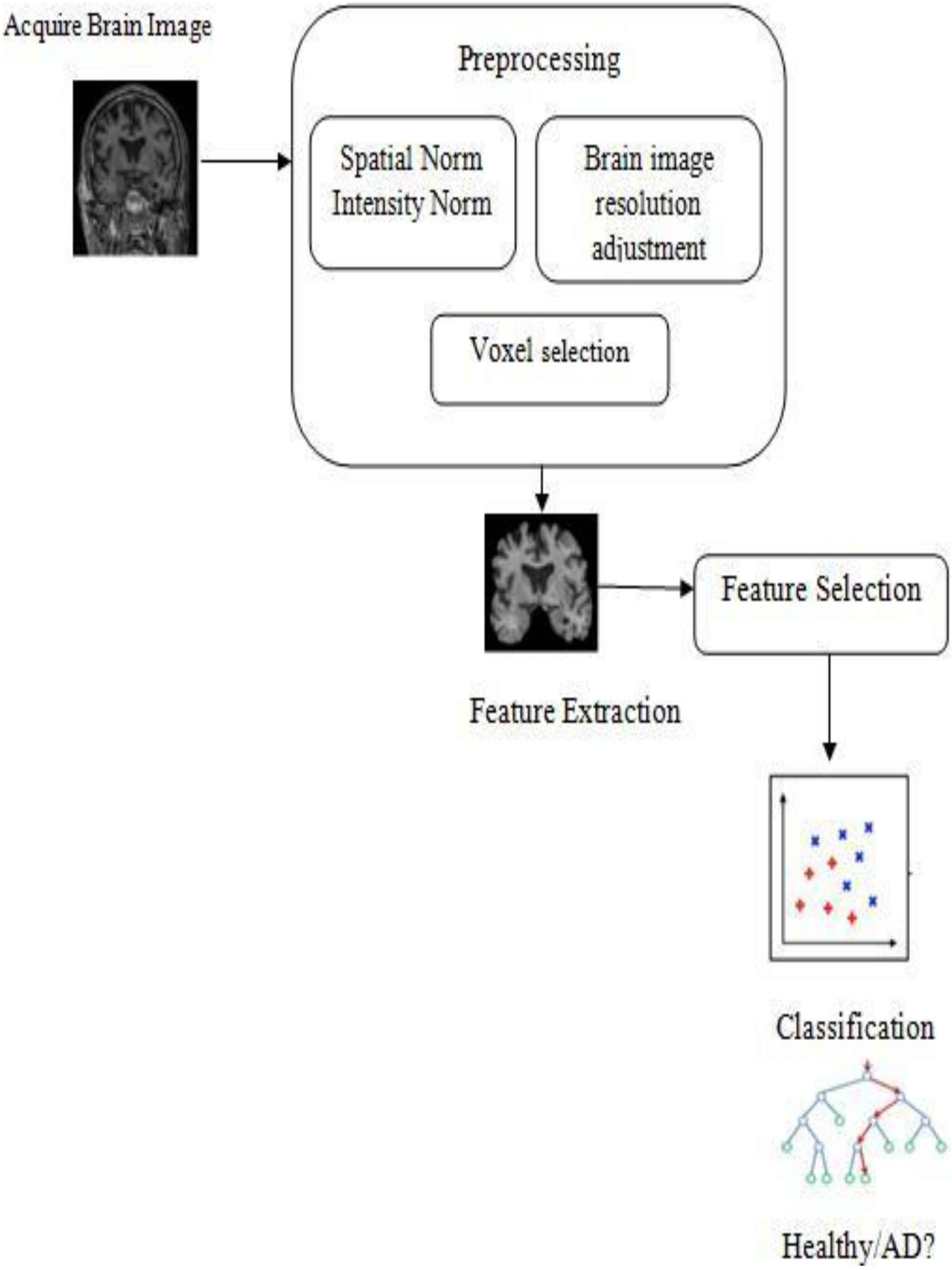


Figure 1 shows a block diagram of the CAD system that consists of four stages: (i) preprocessing, (ii) Feature selection, (iii) feature extraction, and (iv) classification. Most widely used methods for these stages are described in the following sections.

V. CONCLUSION

This paper presents a summary of recent work carried out to classify MRI volumes of AD patients and normal subjects. It also gives an overview of the various stages involved in automatic classification.These stages include preprocessing, feature extraction, feature selection and classification.

REFERENCES

[1] Plant, S. J. Teipel, A. Oswald, C. Böhm, T. Meindl, J. Mourao- Mrna . W od, H apl detection of brain atrophy patterns based on MRI for the rediction lhie‘s *Neuroimage*ies, vol.50,pp.162–174, 2010.

[2] J. Ramírez, J. M. Górriz, D. Salas- Gonzalez, a. Romero, M. López, I. Álvarez, and M. Gómez-í,—optr- aideddiagnosisof Azemr‘ yedmni obndsrmnn *Inf*e.*Sci. (Ny)*f.,vol. etrs||237,pp.59–72, 2013.

[3] L. Khedher, J. Ramírez, J. M. Górriz, a. Brahim, and F. Segovia, —al igoi′disease fbased onlhiepartialleast squares, principal component analysis and support vector machine sn emne*Neurocomputing*R, mgs|| vol.151, pp.139–150, 2015.

[4] A J sbre n -based. morphometry.rso,--the ehd*Neuroimage*, vol. 11, pp. 805–821, 2000.

[5] M. Chupin, E. Gérardin, R. Cuingnet, C. Boutet, L. Lemieux, S. Lhrc, H eai. Greo hipoaps sgetto n lsiid**a**ni**o**inno Azemr‘*Appl. SoftComput.*, volies.11, pp. Ad ml cgiie maret ple2313–2325, 2011n. aa rm DI|| *Hippocampus*, vol. 19, pp. 579–587, 2009.

[6] H asd, —oe o eriaigcasfctoiAzemr‘ fies,lhie‘sih emphasis on brain perfusion SPC.*J* ||*Nucl. Med.*, vol. 48, pp. 1289–1300, 2007.

[7] J. Ben Ali, S. Abid, B. William Jervis, F. Fnaiech, C. Bigan, and M. Bseg, -dniiain- stage Alzheimers disease using fnua N*euro computing*, vol.143, pp. 170–181,[2014]

[8] F. L. Seixas, B. Zadrozny, J. Laks, A. Conci, and D. C. Muchaluat Sae — aein diagnosis of dementia, Alzheimers disease and mild cognitive ipimn*Comput.Biol,.Med.*, vol. 51, pp. 140–58, 2014.

[9] A. Ortiz, J. M. Górriz, J. Ramírez, and F. J. Martínez-Murcia —V-SVM based CAD tool applied to structural MRI for the danss o h*Pattern*lhie‘s*Recognit.Lett.*,vol. 34, pp. 1725–1733, 2013.

[10] N.Bloha n Azemrao; ies *Int*rm.*J.* D SrcuaDelfino, and J.Peña-aaoMI**a**a||Mna aia *Comput. Appl.*, vol. 47, no. 3, pp. 40–44, 2012

[11] R aaoa . a adin n cgiiea Epln, maret—vl**a**dig *Psychiatry*l t**he** Impact of Different Factors on Voxel-Based Classification Methods. O AN tutrl*Int. J.*R*Biomed* . *Data*ri*Min.*, mgs||[27]. Hsn .S aiui .F. J. Martínez- urcia,
J. M. Górriz, J. Ramírez, C. G. Puntonet, and Alzheimr‘ ies- Whitneyae-WilcoxonnU-et||an[28] *Expert Syst. Appl.*, vol. 39, pp. 9676–9685, 2012.

[12] F. J. Martínez-Murcia, J. M. Górriz, J. Ramírez, C. G. Puntonet, and Salas-ozlz —optr Add Dansspp.1062–1072,2011. ol fr

[13] Alzheimr‘ ies-Whitneyae-WilcoxonnU-et||an[28 *Expert Syst. Appl.*, vol. 39, pp. 9676–9685, 2012

[14] R. Chaves, J. Ramírez, J. M. Górriz, and C. G. Puntonet, —soito-ae ueetr eeto ehdfrAzemr‘ ies *Expert*igoi,*Syst.Appl*.vol.39, no. 14, pp. 11766–11774, 2012.

[15] A ak .J ak .Se,adJ u Dtcino lhie‘sdisease by Raman spectra of rat's platelet with a simple feature slcin||*Chemom.Intell. Lab. Syst.*, vol. 121, pp. 52–56, 2013.

[16] H. Matsua Rl fnuomgn nAzemr‘ ies,wt mhsso ri*J. ucl*efso.*Med.*,vol.48,pp. PC.|| 1289–1300, 2007.

[17] F. Segovia, J. M. Górriz, J. Ramírez, D. Salas-González, and I. Ávrz ErydanssonPartialfAzemr‘ ies ae es qae n upr*ExpertSyst.Appl* .etrvol. ahn, 40, no. 2, pp. 677–683, 2013.

[18] J. Ramírez, J. M. Górriz, F. Segovia, R. Chaves, D. Salas-Gonzalez, M e,I lae,adP ail,—optradddansssystem for the lhie‘sdsaebsdo ata es qae n admfrs PC*Neurosci*mg.*Lett.*, vollsiiain||. 472, pp. 99–103, 2010.

[19] I. a. Illán, J. M. Górriz, M. M. López, J. Ramírez, D. Salas-onzalez, F. Segovia, R. Chaves, and C. G. Puntonet, Cmue

[20] Adddansso lhie‘sdsaeuigcmoetbsdSM||*Appl. Soft Comput.*, vol. 11, pp. 2376–2382, 2011.

[21] M. López, J. Ramírez, J. M. Górriz, I. Álvarez, D. Salas-Gonzalez, F. Segovia, R. Chaves, P. Padilla, and M. Gómez-í,—rnia component analysis-based techniques and supervised classification shms fr te ery dtcin o lhie‘s dsae||*Neurocomputing*, vol. 74, pp. 1260–1271, 2011.

[22] M. Termenon, M. Graña, a. Besga, J. Echeveste, and a. Gonzalez- Pno Ltieidpnetcmoetaayi etr eeto ndfuinwihe mgn o lhie‘sdsaecasfcto, *Neurocomputing*, vol. 114, pp. 132–141, 2013.

[23] J. M. Górriz, F. Segovia, J. Ramírez, a. Lassl, and D. Salas- D. Zhang, Y. Wang, L. hu . Ya, ad D ipimn,*Neuroimage*vol. 55, pp. 856– 867, 2011.

[24] D. Schmitter, A. Roche, B. Maréchal, D. Ribes, A. Abdulkadir, M. Bach-Cuadra, A. Daducci, C. Granziera, S. Klöppel, M Maeder,R eryel,ad Gree, -basedA v morphometry for prediction of mild cognitive impairment and A zemr‘*NeuroImage*ies.*Clin.*,vol,7,pp. 7–17, Jan. 2015 ntok eiin

[25] S.J.Sawiak,oeN.I.Wood,oG.B Williams,upriga .J.Morton, and hT.A. Cretr-based morphometryVxl with templates and v vldto n a mue mdl*Magn.Reson.* f H *Imaging*, vol. 31, pp. 1522–1531, 2013.

[26] S. M. Smith, P. Bannister, C. ekan n . Ba dsae||ol o ucinl ad src *Neuroimage*, no. 6, p. 2001, 2001 NBnmae

ENERGY HARVESTING USING PELTIER THROUGH COLD AND HEAT JUNCTION

N. Prabha[#1],Mrs. P. Suthanthira Devi [#2],Mr. A.S. Balaji[#3],Ms. A. Malathi[#4]

[#1]-PG Student, Dept. of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai
[#2,3,4]-Assistant Professor, Dept. of Computer Science and Engineering, Anand Institute of Higher Technology,

Abstract **–The Earth is in trouble, and the release our of greenhouse fault gases. The global demand for electricity is rising. Electricity is vital to modern life. It seems clear at this point that traditional methods of generating electricity are unsustainable, and there is a need to find new energy sources that do not produce as much carbon (or dust off old ones, like natural gas and nuclear power). This need for electricity drives a growing demand for electricity generation Every form of lectricity generation has its strengths and weakness. Non Renewable resources are scarce and exhaustible Large quantities of smoke released into environment causes acid rain, increases greenhouse effect and results in generational birth defects, cancer and other damage. Renewable resources can be replenished from nature but it can be implemented only when there is availability of resources. Future electricity generation will need a range of options, although they must be low carbon Peltier cells are used with very low carbon emissions and relatively small amounts of wastes can be safely stored and eventually disposed of. Voltage can also be generated by means of using Peltier cells. Voltage is generated at two different temperature gradients. It is suited to rural and remote areas and developing countries, where energy is often crucial in human development.**

Keywords—greenhouse effect, Peltier cells, temperature gradient.

I. INTRODUCTION

Mankind has been generating electricity on a industrial scale since 1881. The first powerplants used hydroelectric power and coal power. Since then other methods of power generation have been introduced: natural gas, oil, nuclear, and small amounts of power generated by solar, tidal, wind, and geothermal sources. In 2006, about 15% of global power generation was through nuclear, 16% through hydro, 68% through fossil fuels (coal, oil, natural gas), and less than 1% through renewable (solar, wind, tidal)Power generation involves either transforming heat energy into mechanical energy, such as burning oil or mechanical energy, such as the moving blades of a windmill into electrical energy, using a generator. Even in the case of an advanced power source such as nuclear the heat from fissioning nuclei is used to heat water, which turns a turbine and provides electricity Especially since the 1980s, the Western world has been seeking to decrease its dependency on fossil fuels and increase the use of renewable, but had a little success.

The two primary issues concerning the use of fossil fuel power have been the possible financing of terrorists and Anthropogenic greenhouse gases have been indicated as a major cause of global warming.A non renewable resource(also called a finite resource) is a resource that does not renew itself at a sufficient rate for sustainable economic extraction in meaningful human time frames. An example is carbon-based, organically-derived fuel. The original organic material, with the aid of heat and pressure, becomes a fuel such as oil or gas. Earth minerals and metal ores, fossil fuels (coal, petroleum, natural gas, etc.,) and groundwater in certain aquifers are all non-renewable resources.

Earth minerals and metal ores are examples of non-renewable resources.The metals themselves are present in vast amounts in Earth crust; the processes generally take from tens of thousands to millions of years, through plate tectonics tectonic subsidence and crustal recycling.

There are certain rare earth minerals and elements that are more scarce and exhaustible, high demand in manufacturing. Natural resources such as coal, petroleum (crude oil) and natural gas take thousands of years to form naturally and cannot be replaced as fast as they are being consumed. Coal- Requires around 1.7 million litres of fresh water for each Gigawatt-hour of electricity generated. It produces more carbon dioxide (CO_2) per Watt-hour of energy. Large quantities of ash have to be disposed of and a lot of smoke is produced. When the coal is mined and burned these substances (sulfur, arsenic, selenium, mercury and the radio active elements (uranium, thorium and radium) are released into the environment, which results in acid rain. Natural gas - produces carbon dioxide (CO_2), which is an important greenhouse gas Seismic surveys of the sea bed cause death and injuries to marine species Leakage of methane of the atmosphere to quantify increases the greenhouse effect. The use of nuclear technology requires naturally occurring radioactive material as fuel Uranium, the most common fission fuel, and is present in the ground. This mined uranium is used to fuel energy-generating **nuclear reactors with fissionable uranium-235 which generates** heat that is used to power turbines to generate electricity. The nuclear industry that generates radioactive waste if not properly disposed, is highly hazardous to people and wildlife. Internal or external exposure can cause DNA breakage producing generational birth defects, cancers and other damage.

Renewable energy is generally defined as energy that comes from resources which are naturally replenished on a human timescale such as sunlight, wind, rain, tides, waves, and heat. These resources exist over wide geographical areas. Solar power is obtained from the energy of the sun. Solar technologies use the sun's energy and light to provide heat, light, hot water, electricity, and even cooling. The energy from the sun is not always available. Photovoltaic solar cells directly convert sunlight into electricity. Concentrating solar power is a technology that uses reflective materials like mirrors to concentrate the energy from the sun. The heat energy obtained can be converted to electricity.

Bio-energy technologies use renewable biomass resources -wood, waste and agricultural waste (like corn cobs and wheat straw) - to produce different types of energy, like electricity, liquid, solid and gaseous fuels. Biomass, biogas and bio-fuels are burned to produce heat/power and in doing so harm the environment. Pollutants such as sulphurous oxides (SO_x), nitrous oxides (NO_x) are produced and premature deaths are caused by air pollution. Airflows can be used to run winds turbines. The power available from the wind is a function of the wind speed, so as wind speed increases, power output increases up to the maximum output for the particular turbine. Areas where winds are stronger and more constant, such as offshore and high altitude sites are preferred locations for wind farms.

II. MOTIVATION OF RESEARCH

The motivation of my research is to generate voltage by means of Peltier cells and to monitor the temperature gradient and maintain it within the saturation point.

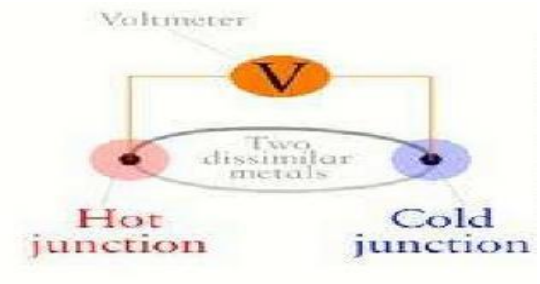
III. PELTIER CELLS

A Peltier element is a simple tool that has no moving parts and can be used to heat or cool or generate electricity. These devices are useful for long time survival situations. Peltier cell is a thermoelectric device. Thermoelectric device is the one which generates voltage when there is a different temperature on each side. These devices consist of two sides Hot and Cold. Peltier cells are commonly constructed of larger amount of semiconductor elements. Join two dissimilar metals by two separate junctions, and maintain the two junctions at different temperatures, a small voltage develops This method of generating voltage include, durability, flexibility and user safety i.e., free from shock and free from noise compared to generator. It is suited to rural and remote areas and developing countries, where energy is often crucial in human development. Peltier cells are used with very low carbon emissions and relatively small amounts of waste can be safely stored and eventually disposed of.

IV. VOLTAGE GENERATION

Peltier elements are mainly made of semi-conductive material. This means that they have P-N contacts within. Actually, they have a lot of P-N contacts connected in series. They are also heavily doped. These Two metals are connected at different temperature gradient and wire coming out of this cell is connected to voltmeter. Voltage generated is measured by means of using voltmeter.

Fig.1. Generation of voltage at different temperature gradient



V. PELTIER POWER

Array of Peltier cells are placed in between the temperature difference (heat & cold) and the voltage is produced. This DC voltage is converted to pure DC and boosted into DC voltage and stored in battery for future use. By means of microcontroller the temperature sensor and cooler DC motor has been connected. If the heat goes above the saturation point the cooler DC motor is switched on automatically and reduces the heat. The continuous temperature of heat is displayed by means of using LCD display and heat is monitored by temperature sensor.

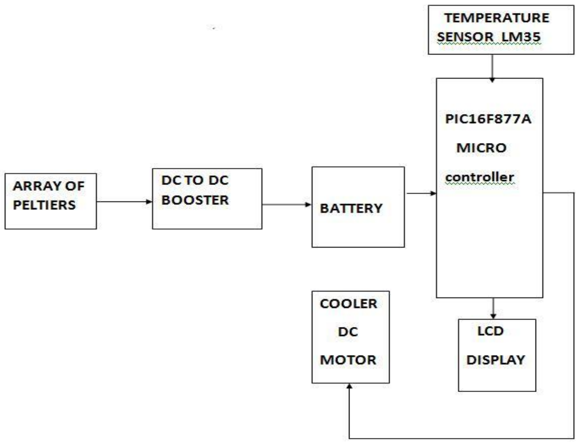


Fig. 2 . Block diagram of experimental arrangement

VI. TEMPERATURE MONITORING

A transformer is a static electrical device that transfers energy by inductive coupling between its winding circuits. A varying current in the primary winding creates a varying magnetic flux in the transformer's core and thus a varying magnetic flux through the secondary winding. This varying magnetic flux induces a varying electromotive force (EMF), or "voltage", in the secondary winding. When used in its most common application, for conversion of an alternative current(AC) input into a direct current (DC) output, it is known as a bridge rectifier.

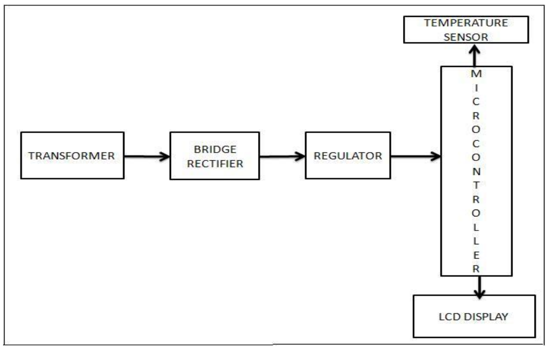
A bridge rectifier provides full-wave rectification from a two-wire AC input, resulting in lower cost and weight as compared to a rectifier with a 3-wire input from a transformer with a center-tapped secondary winding Here is a 5V power supply circuit using LM 7805 IC. LM7805 is a famous positive voltage regulator IC comes in three terminals provides fixed 5V DC output. This IC has many built in features like internal current limiting, thermal shut down, operating area protection etc. Fig.3. Continuous monitoring of temperature using temperature sensor IC will become hot during the operation so it is essential to use a good heat sink. In fig[4], as the temperature gradient increases voltage generation also increases. There should be a change in temperature difference to produce the voltage. Voltage produced is directly proportional or dependent based on the temperature difference of the Peltier cell.

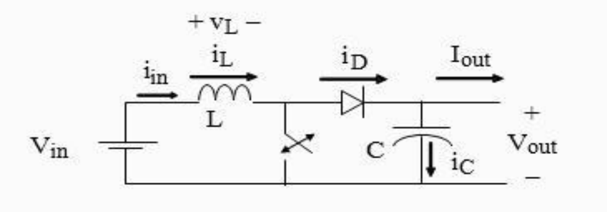
VII. CONVERTER

If the MOSFET gate drives position, then there is a short circuit through the MOSFET – blow MOSFET. If the load is disconnected during operation, so that $I_{out} = 0$, then L continues to push power to the right and very quickly charges C up to a high value (250V) –blow diode and MOSFET

Before applying power, make sure that your D is at the minimum, and that a load is solidly connected. Buck, Boost, Buck-Boost, Cuk transfer energy in only one direction full-bridge is capable of bi-direccional power flow in Buck, Boost, switch utilization is good in Buck-Boost, Cuk, full-bridge switch utilization is poor.

Fig. 4. Voltage produced by peltier at different temperature gradient





VIII. EXPERIMENTAL RESULTS

Peltier generates more Watts than sollar cells. A standard solar panel will normally put around12 –17v at ideally 100 watts. If the Peltier cells are connected as a panel 3686watts can be produced.

IX. CONCLUSION

Peltier cells along with temperature sensor maintains the heat on one side within the saturation point. So if the heat goes above the saturation point voltage generation is stopped. Cooler DC motor brings the heat below the saturation point and maintains the voltage generation. Producing energy depends on the maximum number of cells used. If the usage of Peltier cells are more then voltage generation will be increased.

REFERENCES

[1] F. Herrmann, Handbook“Curof Applied Superconductivity, B. Seeber, Ed. Philadelphia, PA, USA: Institute of Physics Publishing, 1998, ch. D10, pp. 801–843.

[2] Yamaguchi *et al.*, “Refrigera realize multistage and gas-cooled Current lead,”*IEEEAppl. Supercond.*, vol. 23, no. 3, Jun. 2013, Art. ID. 4802304.

[3] McFee, “Optimum i apparatus,” *RevSci. Instrum.*, vol. 30, no. 2, pp. 98– 102, Feb. 1959.

[4] L. Haugan, J. D. Long, A. Hampton, and P.N. Barnes, “Designight power transmission devices for specialized high power applications, ”Power Systems Conf., Washington, DC, USA, 2008.

[5] O’Rourke,-drivepropulsion“ElectrforU.S. Navy ships: Background and issues for congress,” nal Congressi Research Service Report for Congress, Washington, DC, USA, RL30622, Jul. 31, 2000.

[6] T. Kephart *et al.*, “High tem conducting degaussing from feasibility study to fleet adoption, ”*IEEE Trans. Appl. Supercond.*, vol. 21, no. 3, pp. 229–2232, Jun. 2011.

[7] Yamaguchi *et al.*, “Peltier experiment and Their applications for super conducting *Rev. Sci. Instrum*magn., vol. 75, pp. 207– 212, 2004.

[8] Bromberg, P. C. Michael, J. V. Minervini, and C Miles, optimization “Currfor cryogenic operation at intermediate temperatures,”*Proc. AIPConf.* 2010 a, in vol. 1218, pp. 577–584.

CONTROLLING DRIVING SYSTEM USING BLUE EYES TECHNOLOGY

S.Brindha[#1] , S.Thilagavathi*[2] M.Kalaivani**

[#1]*Dhanalakshmi College of Engineering*

[*2]*Dhanalakshmi College of Engineering*

**Assistant Professor,Dhanalakshmi College of Engineering

***Abstract* - Blue eyes technology can be used in controlling the driving systems to reduce the number of accidents happening in the world. It follows the concept of emotional mouse and affective computing. A sensor is attached to the steering wheel and it can access the emotional stability of the driver and guide him in traffic conditions. The main objective of this paper is to enable the perceptions in the machine by using natural inputs like human emotions .This technology has a power to change the future of the world. When a driver is very angry, not emotionally stable, stressed and the driver is increasing his speed of the vehicle, then this technology can detect it and reduce the speed, or use auto-drive mode stating the emotional instability of the driver and help him drive back safely .It Proper exceptions should be implemented for situations like emergency or in case of ambulance to not make the technology look like a hindrance to the driver. Also they can be used to alert the users who are drowsy or sleepy during driving.**

***Index Terms* - Blue eyes technology, emotional mouse, affective computing.**

I. INTRODUCTION

Human cognition depends on highly developed abilities to perceive, integrate and interpret visual, auditory and touch information. If such perceptions are added to computers even in a small fraction, definitely computers would become even more powerful than they are today. Also they can help human beings in much more better manner. Blue Eye aims at creating the perceptual and sensual abilities tocomputers. IBM scientists, at Almaden Research Center (ARC) in San Jose, the main IBM research laboratory, are trying to enable the computers to listen to our speech, sense our gaze and read our body language since 1997.

Affective Computing is computing that relates to, arises from, or deliberately influences emotion or other affective phenomena. Affective Computing research combines engineering and computer science with psychology, cognitive science, neuroscience, sociology, education, psychophysiology, value-centred design, ethics, and more.

The various steps involved in affective computing are

1. Adding sensory ability to computers.
2. Detecting the emotions of human being.
3. Respond accordingly.

They are trying to enable these senses to computers with the help of video cameras, speech recognition technology, gaze tracking systems, facial geometry to detect expressions etc to gather key information. This information is then analysed to determine the user's physical, emotional, or informational state, which in turn can be used to help make the user more productive by performing expected actions or by providing expected information. The exciting science fiction of being able to tell our computer what it should do is not far away from being reality with the help of these technologies in place.

Machines then can act according to the commands received from the users by their senses rather than requiring user to be present physically present before the system and enter the various commands to execute the desired action. For example, ask the computer for a search in Google, turn on music or turn off, make a phone call for you etc, or even better computers can sense your emotional state and try reacting accordingly like trying to play your favourite music when you are tensed or little low etc.

In the future, ordinary household devices -- such as televisions, refrigerators, and ovens -- may be able to do their jobs when we look at them and speak to them. The input from the user is a touch for ex emotional mouse.

The basic idea behind this is to fix an Emotional Mouse to the steering wheel of the car. The mouse developed to evaluate the emotional state of the user such as anger, fear, sadness, disgust, happiness, surprise etc when the computer is used. The information the emotional mouse can detect is of two types

- Behavioral
  - Mouse movements.
  - Button click frequencies
  - Finger pressure when the user presses his/her button.
- Physiological
  - Heartrate(Electrocardiogram,Photoplethysmogram)
  - Skin temperature(Thermester)
  - Skin electricity(Galvanic skin response)
  - Electromyographic activity(Electromyogram)

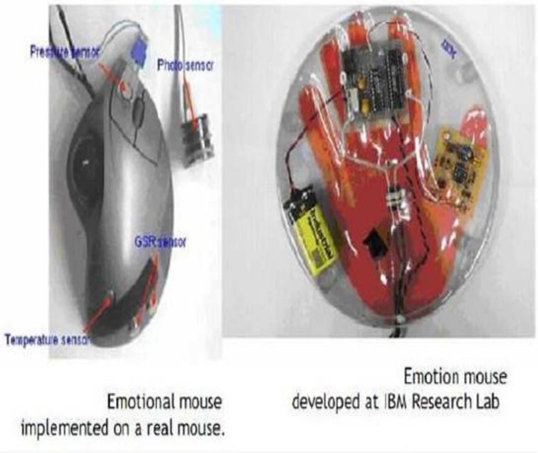

Pressure sensor
Photo sensor
GSR sensor
Temperature sensor
Emotional mouse implemented on a real mouse.
Emotion mouse developed at IBM Research Lab

Fig.1 Implementation of Emotional Mouse

The emotional mouse is designed with an objective to measure the physical and physiological data without user's perception or obstruction as much as possible.

II. Blue Eye Technology

Blue Eyes uses non-obtrusive sensing technology, such as video cameras and microphones, to identify and observe a user's actions, and to extract key information, such as where the user is looking and what the user is saying verbally and by gesture. These cues are analysed to determine the user's physical, emotional, or informational state, which in turn can be used to help make the user more productive by performing expected actions or by providing expected information.

Data Acquisition System is used to get the analog data from the sensors of the emotional mouse. Emotions are mapped to the sensor outputs using a correlation model. The correlation model is derived from a calibration process in which a baseline attribute-to-emotion correlation is rendered based on statistical analysis of calibration signals generated by users having emotions that are measured or otherwise known at calibration time. From the information obtained, emotional state of the user and the activity he is currently involved in can be related as information about the user. A variation of emotional mouse called the sentic mouse has also been tested to identify directional pressure sensor which would interpret the likings or disliking.

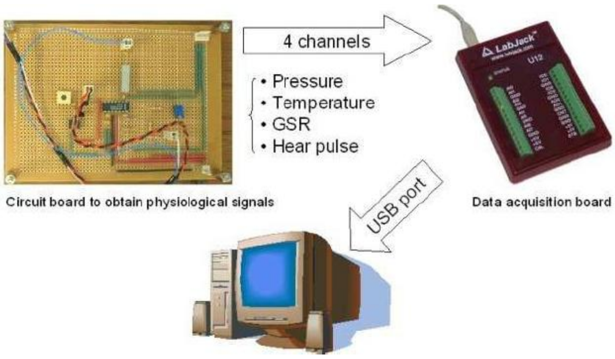


Fig. 2 Data Acquisition System

III. Architecture

There are basically four sensors used for measuring the pressure, temperature, galvanic skin response (GSR) and the heart rate. Heart rate is taken by IR on the thumb, temperature is taken using a thermistor chip, GSA is taken through the mouse device driver, and GSR is taken through fingertips. These values are input into a series of discriminate function analyses and correlated to an emotional state. In addition to this we use two other sensors fitted to the head lights. They are velocity sensors and gyro sensors.

Specifically, for the mouse, discriminate function analysis is used in accordance with basic principles to determine a baseline relationship, that is, the relationship between each set of calibration physiological signals and the associated emotion.

To be included in the discriminate function analysis, the proportion of each signal's emotion-specific variance (that is not accounted for by other non-excluded signals) to total variance must exceed a criterion proportion, which for the mouse is 0.001 (or one part per every thousand). After any signals are excluded from the analysis, all signals are analyzed simultaneously to describe the baseline relationship by a number of discriminate functions equal to one less than the number of emotions sought (N-1) or the number of physiological signals, whichever is less.

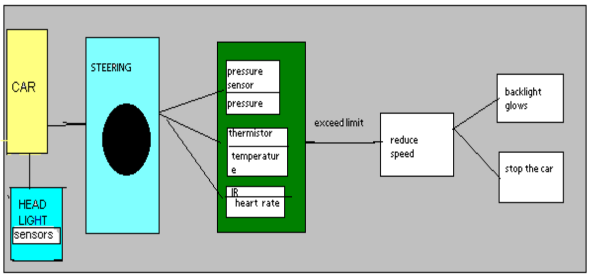


Fig. 3 Architecture diagram

IV. Working

The working goes as follows. The steering wheel incorporates sensors. These sensors take the inputs of temperature, pressure GSR and the heart rate. The sensors monitor vital signs and stress levels certain metrics. The metrics are heart rate and blood oxygen saturation. The steering system takes measures to reduce distractions or slow down the vehicle. The vehicle has to detect when the driver is no longer feeling well and to initiate appropriate measures. When a stress situation is detected by means of skin conductance values, phone calls can be blocked, for instance, or the volume of the radio turned down automatically and mainly the speed of the vehicle can be reduced. With more serious problems the system could turn on the hazard warning lights, reduce the speed or even induce automated emergency braking. This is mainly used in the case when the driver is facing some serious problems. For example, when the driver falls sick or he has got low BP or any other medical disorder.

The sensors are fitted into the steering wheel of the vehicle. This will enable the driver control the driving system. That is in the case of any medical emergency or any other issues the driver may raise the speed of the vehicle. This will lead to many road accidents. To avoid such a situation this emotional steering will come into the frame. When the driver tries to increase the speed of the vehicle, this system will automatically reduce the speed of the vehicle thereby controlling the entire driving systems.

Fig. 4 Inner section of a car steering wheel

Along with the head lights the gyro sensors and velocity sensors are fitted. Vehicles with a navigation system onboard use among other sensors a gyro sensor. This gyro sensor, together with a velocity sensor, could be used to compute the driving trace in real time. The result of the calculation with gyro sensor is in fact very similar as the one with use of a lateral vehicle position detection system, with the great advantage that sensors already present in the vehicle can be used.

The driving systems are controlled by the steering under the following circumstances,

1. When the input to the pressure sensor is above the average pressure level of a normal human being.

   i.e. when the systolic pressure is above 120-130 Hg and the diastolic pressure is below 80-70 Hg.

2. When the input to the thermistor chip(used to measure the temperature) is above 97.9°F .
3. When the input to the IR sensors(used to measure the heart rate) is not between 60-100 beats per minute.

V. Mood Measurement Methods

A. *Physiological*

There is evidence in literature suggesting that physiological signals have characteristic patterns for specific affective states (e.g. Ekman et al., 1983). Several studies have even provided evidence for a correlation between physiological variables and the affective dimensions of valence and arousal (e.g. Lang et al., 1993, Gomez & Danuser, 2002), thus 4 suggesting that emotion is fundamentally organized by these two parameters. Physiological signals such as skin conductance, heart rate, blood pressure, respiration, pupillary dilation, electroencephalography (EEG) or muscle action potentials can provide information regarding the intensity and quality of an individual’s internal affect experience. In our experiment, we used a combination of physiological signals as a primary source to verify self-assessment results of affect, also because it was possible to get data simultaneously with the task performed.

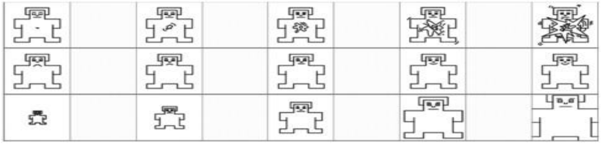
B. *Behavioural*

There exists a broad field of behavioural methods for the measurement of affect: facial expressions, voice modulation, gestures, posture, cognitive performance, cognitive strategy, motor behaviour (e.g. hand muscles, head movement), etc. Behavioural measurement methods5 are based on the fact that the body usually responds physically to an emotion (e.g. changes in muscle tension, coordination, strength, frequency) and that the motor system acts as a carrier for communicating affective state. Especially promising for these methods is that humans also use many of these signals in everyday life to judge the affective state of other people.

In contrast to physiological methods can behavioural methods be applied in a non-invasive way (although video cameras used in face recognition may be considered obtrusive). There are also a few existing projects dealing with motor behaviour in HCI, e.g. the analysis of mouse clicking behaviour after frustrating events during a computer task (Scheirer, 2002), where 4 distinct patterns of mouse clicking could be found or the visual comparison of mouse movement patterns on a e-commerce site for user modelling (Lockerd & Mueller, 2001).

Based on these moods of the driver the driving system will be controlled by the sensors fitted to the steering wheel.

Fig. 5 Mood Measurements



VI. Applications

A. *Assisting Human Operators*

By monitoring and recording the operator’s physical condition. In the complex industries like chemical industry or nuclear sector where exists danger in the environment of exposure to toxic substances or radiations, monitoring helps the human operators. The operator has to raise the alarm by himself by announcing the danger he is input with the help of these systems, the technology keeps an eye on the operator for normal conditions. If any parameter is found in abnormal conditions like a raise in pulse rate or low level of oxygenation then an alarm can be triggered automatically.

B. *Medical supervision*

It is possible with this technology. It can help the doctor in concentrating more on his work than getting distracted for putting down all the observations he is making. He can go through data of many patients and then just tell the computer to make note of the observations he is making through voice instructions. This helps especially in case of x-rays, scans etc. Monitoring of patients can be done by detecting the physiological conditions of him/her like blood pressure, pulse rate, oxygenation. The position of the person can be determined like whether the person is sitting or standing or lying down

The technology on its successful implementation has got limitless application in every possible industry out there in the world. Interactive environment will be built where anything is possible without making the user feel that the technology is actually complex in nature. Till today the technology advancement has required the users to adapt themselves to the technology by dedicating time to learning what it is all about, making them feel they are ignorant of it. This new technology actually will make the user more comfortable.

VII. Conclusions

It prevents the user from dangerous incident. It also minimizes the ecological consequences. It is the system developed, intended to be the complex solution for monitoring and recording the operator’s conscious brain involvement as well as his physiological condition. Human are prone to error. They are not perfect, they fail drastically at times. A small mistake committed unintentionally can cause a disaster for them.

Machines can be helpful in preventing the mistakes and correcting the errors of human. The opinion about machines as being complicated and difficult to handle will be changed by blue eyes. User friendliness is increased in computing devices making the life more convenient and simple possible. The gap between the physical and electronic world can be minimized to a bare minimum

The blue eyes technology aims at creating computational machines that have perceptual and sensory ability like those of human beings. In the near future, ordinary household devices- such as television, refrigerators, and ovens may be able to do their jobs when we look at them and speak to them. Future applications of blue eye technology is limitless

REFERENCES

[1] Eskandarian and R. Sayed, “Driving Simulator Experiment: Detecting Driver Fatigue by Monitoring Eye and Steering Activity,” Proc. of NDIA Symp. on Annual Intelligent VehiclesSystems,June2003.

[2] R. Grace, V.E. Byrne, D.M. Bierman, J.-M. Legrand, D. Gricourt, B.K. Davis, J.J. Staszewski and B. Carnahan, “A Drowsy Driver Detection System for Heavy Vehicles,” Proc. Of AIAA/IEEE/SAE 17th DASC Conf. on Digital Avionics Systems, vol.2, pp.I36/1-I36/8, 31 Oct.-7 Nov. 1998.

[3] P. Smith, M. Shah and N. da Vitoria Lobo, “Monitoring Head/Eye Motion for Driver Alertness with One Camera,” Proc. of 15th Int'l Conf on Pattern Recognition, vol.4, pp. 636-642, Barcelona, Spain, Sept. 2000.

[4] A. Vuckovic, V. Radivojevic, A. C. N. Chen and .Popovic,“Automatic Recognition of Alertness and Drowsiness from EEG by An Artificial Neural Network,” Journal of Medical Engineering & Physics, vol.24, no.5, pp.349-360, June 2002.

[5] R.L. Hsu; A. M. Mottaleb and A. K. Jain, “Face Detection on Color Images, ”

Controlling Vampire Attacks in Wireless Sensor Networks

K.M.Kashifa Thabasum[#1], G.Nandhini[*2],A.Malathi[*3]

[#1,*2] *UG Student, Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai.*
[*3]*Assistant Professor, Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai.*

nandynarma@gmail.com

***Abstract*- Ad hoc wireless sensor networks continually proves to exist as an exciting domain in carrying out various research activities and also has varied applications worldwide. However, the more promising it is, the more threats it carries with respect to its security. One such threat is a new class of resource depletion attacks often called as vampire attacks which drain the node's battery power and disable the network permanently. Much spotlight is given on this class of attacks as we will discuss two variations of vampire attacks along with a proof of concept protocol put forth by Parno, Luk, Gustad, Perrig (PLGP) which bounds the damage caused by vampire during the packet forwarding phase. But PLGP fails to offer a satisfactory solution during the network topology discovery phase. In this paper, we discuss methods to secure the discovery phase and prevent the occurrence of vampire attacks through an enhanced DSDV protocol.**

I. INTRODUCTION

Wireless sensor networks promises new and diverse applications in the future which includes fields like environmental monitoring, agricultural monitoring, machine health monitoring, surveillance and medical monitoring. These networks, which connect the physical world with the digital world, provide us with a richer understanding of our environment and with the ability to more accurately control our surroundings. However, there are many challenges that must be addressed before the full potential of these networks are realized. Wireless sensor networks must be reliable and scalable to support large numbers of unattended wireless sensors; they must last for extended periods of time using limited battery power;

They must be secure against outside attacks on the network and on data fidelity; they must be accurate in providing required information while performing in-network processing to reduce data load; and they must interface with existing networks. While these schemes can prevent attacks on the short-term availability of a network, they do not address attacks that affect long-term availability—the most permanent denial of service attack is to entirely deplete nodes' batteries. This is an instance of a resource depletion attack, with battery power as the resource of interest. In this paper, we consider how routing protocols, even those designed to be secure, protection from these attacks, which we call Vampire attacks, since they drain the life from networks nodes. These attacks are distinct from DoS, reduction of quality (RoQ), and routing infrastructure attacks as they do not disrupt immediate availability, but rather work over time to entirely disable a network.

Vampire Attacks

We define a Vampire attack as the composition and transmission of a message that causes more energy to be consumed by the network than if an honest node transmitted a message of identical size to the same destination, although using different packet headers. We measure the strength of the attack by the ratio of network energy used in the benign case to the energy used in the malicious case, i.e., the ratio of network-wide power utilization with malicious nodes present to energy usage with only honest nodes when the number and size of packets sent remains constant. Safety from Vampire attacks implies that this ratio is 1.

Energy use by malicious nodes is not considered, since they can always unilaterally drain their own batteries.and moreover they are not protocol-specific, in that they do not rely on design properties or implementation faults of particular routing protocols, but rather exploit general properties of protocol classes such as link-state, distance-vector, source routing, and geographic and beacon routing. Neither do these attacks rely on flooding the network with large amounts of data, but rather try to transmit as little data as possible to achieve the largest energy drain, preventing a rate limiting solution. Since Vampires use protocol-compliant messages, these attacks are very difficult to detect and prevent.

Overview

In this paper, we present two variations of increasingly damaging Vampire attacks, one called as the carousel attack, where there are purposely intended loops and the packets move in circles without reaching the intended destination node. It targets source routing protocols by exploiting the limited verification of message headers at forwarding nodes, allowing a single packet to repeatedly traverse the same set of nodes. Much has been discussed about this attack but no countermeasures were provided. The second one called the stretch attack, where the path chosen for the packet to traverse is usually longer than the optimal path possibly traversing the entire network. It also targets source routing protocol and increases packet path lengths, causing packets to be processed by a number of nodes that is independent of hop count along the shortest path between the adversary and packet destination. A single attacker can use a carousel attack to increase energy consumption by as much as a factor of 4, while stretch attacks depends on the position of malicious nodes.

When both these attacks are combined, the number of adversarial nodes in the network increases, thereby causing a big impact on the network. While carousel attack is simple to prevent with negligible over-head, the stretch attack is far more challenging. We evaluate their vulnerability, their aftermaths and suggestions for tackling them. We next discuss the PLGP protocol taken from the model by Eugene and Nicholas.

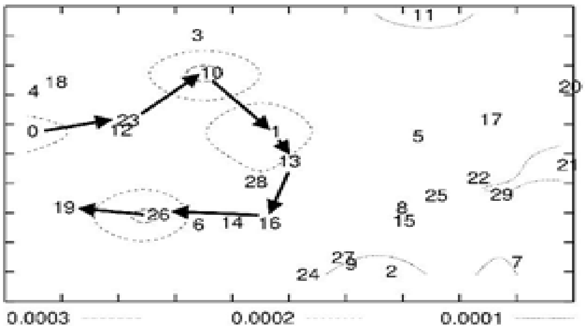
This protocol bounds the damage caused during the packet forwarding phase. We then show how an adversary can target not only packet forwarding phase but also route and topology discovery phases—if discovery messages are flooded, an adversary can, for the cost of a single packet, consume energy at every node in the network which has proved to be a drawback in the case of PLGP protocol. In the later part of this paper, we discuss the DSDV protocol which is table driven and how it can be enhanced to prevent the damage which can arise during the topology discovery phase.

1. Attacks on Source Routing Protocol

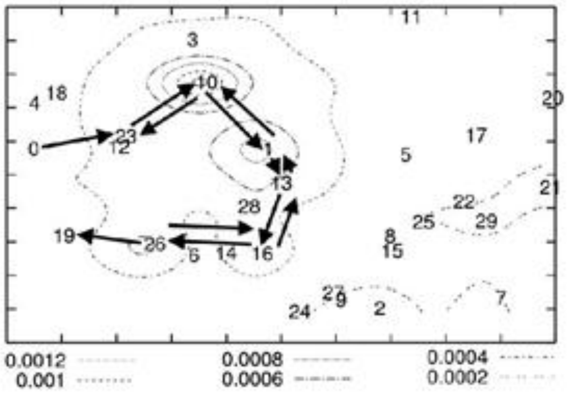
In this section, the carousel and stretch attacks are evaluated using a randomly generated network topology consisting of 30 nodes and a single randomly generated DSR agent, using the ns-2 network simulator.

1.1 Carousel Attack

In this attack, an adversary sends a packet with a route composed as a series of loops, such that the same node appears in the route many times which appears to be cyclic. This strategy can be used to increase the route length beyond the number of nodes in the network, only limited by the number of allowed entries in the source route. The same can be explained with the help of a diagram.



(a) Honest scenario: node 0 sends a single message to node 19.



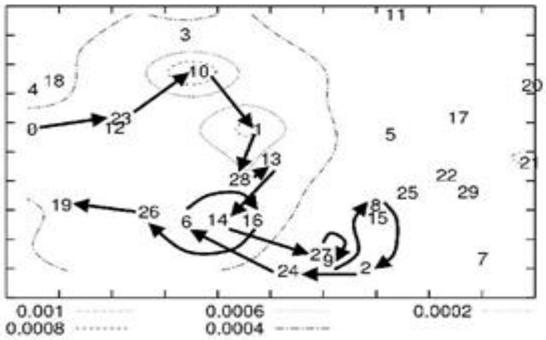
(b) Carousel attack (malicious node 0): the nodes traversed by the packet are the same as in (a), but the loop over all forwarding nodes roughly triples the route length (the packet traverses the loop more than once). Note the drastically increased energy consumption among the forwarding nodes.

In the first diagram (a), the source node 0 transmits the message to the destination node 19 using the shortest optimal path in the topology. This is called an honest scenario. In the second diagram, the node 0 transmits the message to the destination node 19 but this time the source node becomes malicious and generates loops along the traversal path causing a tremendous increase in the energy of the network. There are many circular loops formed at node 10,1,16 and 26.

Assuming the adversary limits the transmission rate to avoid saturating the network, the theoretical limit of this attack is an energy usage increase factor of O(n) where n is the maximum route length. Overall energy consumption increases by up to a factor of 3.96 per message. On an average, a randomly located carousel attacker in the example topology can increase network energy consumption by a factor of 1:48 ± 0:99. The reason for this large standard deviation is that the attack does not always increase energy usage—the length of the adversarial path is a multiple of the honest path, which is in turn, affected by the position of the adversary in relation to the destination, so the adversary’s position is important to the success of this attack.

1.2 Stretch Attack

In this type of attack, the malicious node constructs paths to transmit the message to the destination node (which may be an honest one) which are far longer than the optimal path in the topology. These artificial routes can cause nodes that do not lie along the honest route to consume energy by forwarding packets they would not receive in honest scenarios. Due to this, they get to lose their own energy. This can be explained with the help of a diagram.

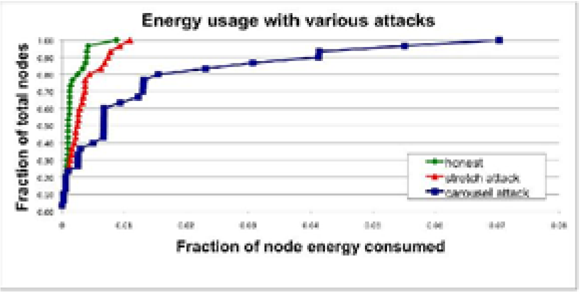


(c) Stretch attack (malicious node 0): the route diverts from the optimal path between source and destination, roughly doubling in length. Note that while the per-node energy consumption increase is not as drastic as in (b), the region of increased energy consumption is larger. Overall energy consumption is greater than in the carousel attack, but spread more evenly over more network nodes.

Comparing the diagram(c) with (a), the latter one is of an honest scenario where node 0 transmits a message to node 19 using the best optimal path available in the network topology. However in the former diagram(c), the malicious node constructs artificial long paths starting from the node 28 where a diversion takes place to nodes 13, 14, 27, 9, 8, 15, 2, 24 and 6 no longer using the optimal path.

1.3 Comparison

On comparing the usage of energy in the network by various attacks we observe the following, The energy usage of carousel attacks is higher compared to other attacks because in carousel attack, the nodes along the shorter path only are affected. In contrast, the energy consumption due to stretch attack is somewhat uniform in the network because the traversal route is increased making most of the nodes in the topology spend their energy and process the packet.



The resource utilization was independently computed for honest nodes and malicious nodes and was found that the malicious nodes did not use a disproportionate amount of energy in carrying out the attack. In other words, malicious nodes are not driving down the cumulative energy of the network purely by their own use of energy. The theoretical limit of the stretch attack is a packet that traverses every network node, causing an energy usage increase of factor O(min(N, λ)), where N is the number of nodes in the network and λ is the maximum path length allowed. This attack is potentially less damaging per packet than the carousel attack, as the number of hops per packet is bounded by the number of network nodes. However, adversaries can combine carousel and stretch attacks resulting in a "stretched cycle" where the packet travels in long paths and takes circular loops as well. Therefore, even if stretch attack protection is not used, route loops should still be detected and removed to prevent the combined attack. Not all routes can be significantly lengthened, depending on the location of the adversary. Unlike the carousel attack, where the relative positions of the source and sink are important, the stretch attack can achieve the same effectiveness independent of the attacker's network position relative to the destination, so the worst case effect is far more likely to occur.

Both these attacks are less effective in hierarchical networks due to the presence of aggregators. In hierarchical networks, the nodes send messages to aggregators, who in turn send them to other aggregators, and they route it to the monitoring point. The described carousel and stretch attacks are valid only within the network neighbourhood of the adversarial node. If an adversary corrupts nodes intelligently or controls a small but non-trivial portion of nodes, it can execute these attacks within the individual network neighbourhoods. A single adversary per neighbourhood is enough to disable the entire network.

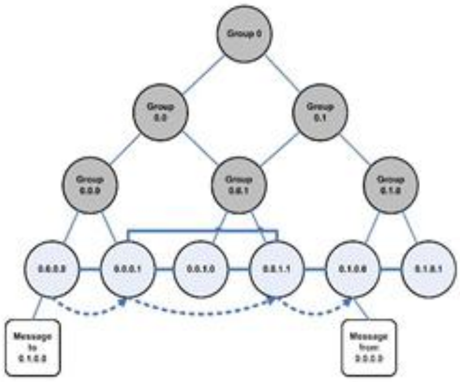
1.4 Countermeasures

The carousel attack can be prevented when the nodes that are responsible for forwarding the message are enabled with mechanism to check the source routes for loop. But it comes with the cost of extra forwarding logic and more overhead, yet it is worthwhile in malicious environments. The ns-2 DSR protocol implements loop detection, but confusingly does not use it to check routes in forwarded packets. When a loop is detected in the network, the source route is corrected and the packet is sent on, but one of the attractive features of source routing is that the route can itself be signed by the source. Therefore, it is better to simply drop the packet, especially considering that the sending node is likely malicious (honest nodes should not introduce loops). An alternate solution provided is to alter the processing of message by the intermediate nodes. To forward a message, a node must determine the next hop by locating itself in the source route. If a node searches for itself from the destination backward instead from the source forward, any loop that includes the current node will be automatically truncated (the last instance of the local node will be found in the source route rather than the first). No extra processing is required for this since a node must perform this check anyway.

Alternatively, the damage of carousel and stretch attackers can be bounded by limiting the allowed source route length based on the expected maximum path length in the network, a way to determine the network diameter is needed. While there are suitable algorithms there has been very little work on whether they could yield accurate results in the presence of adversaries. If the number of nodes is known ahead of time, graph-theoretic techniques can be used to estimate the diameter. Rate limiting may initially seem to be good but later was found that it was not ideal. It limits malicious sending rate, potentially increasing network lifetime, but that increase becomes the maximum expected lifetime, since adversaries will transmit at the maximum allowed rate. Moreover, sending rate is already limited by the size of nodes' receive queues in rate-unlimited networks. Rate limiting also potentially punishes honest nodes that may transmit large amounts of time-critical data, but will send little data over the network lifetime.

Clean state sensor network routing

A clear slate sensor network routing protocol proposed by Parno, Luk, Gustad and Perrig(called PLGP), is modified to resist Vampire attacks during the packet forwarding phase in this section. It was originally developed for security but is vulnerable to Vampire attacks. This PLGP protocol consists of two phases a topology discovery phase, followed by a packet forwarding phase, with the former optionally repeated on a fixed schedule to ensure that topology information stays current. This protocol is explained with the help of a diagram,



1.5 Topology Discovery Phase

PLGP begins with the discovery of the network topology where a tree is formed which is used as an addressing scheme. When discovery begins, each node has a limited view of the network—the node knows only itself. It is a time-limited period during which every node must announce its presence by broadcasting a certificate of identity, including its public key (referred to as node ID), signed by a trusted offline authority. Each node starts as its own group of size one, with a virtual address 0. Nodes who overhear presence broadcasts form groups with their neighbours. When two individual nodes (each with an initial address 0) form a group of size two, one of them takes the address 0, and the other becomes 1. Groups merge preferentially with the smallest neighbouring group, which may be a single node. Like individual nodes, each group will initially choose a group address 0, and will choose 0 or 1 when merging with another group. Each group member prepends the group address to their own address, e.g., node 0 in group 0 becomes 0.0, node 0 in group 1 becomes 1.0, and so on. Each time two groups merge, the address of each node is lengthened by 1 bit. Implicitly, this forms a binary tree of all addresses in the network, with node addresses as leaves.

At the end of discovery, each node learns every other node's virtual address, public key, and certificate, since every group members knows the identities of all other group members and the network converges to a single group. Each node computes the same address tree as other nodes. All leaf nodes in the tree are physical nodes in the network, and their virtual addresses correspond to their position in the tree (as given in the diagram). All nodes learn each other's virtual addresses and cryptographic keys. The final address tree is verifiable after network convergence, and all forwarding decisions can be independently verified. Furthermore, assuming each legitimate network node has a unique certificate of membership (assigned before network deployment), nodes who attempt to join multiple groups, produce clones of themselves in multiple locations, or otherwise cheat during discovery can be identified and evicted.

1.6 *Packet Forwarding Phase*

During the packet forwarding phase, all decisions are made independently by each node. When receiving a packet, a node determines the next hop by finding the most significant bit of its address that differs from the message originator's address (shown in the diagram). Thus, every forwarding event (except when a packet is moving within a group in order to reach a gateway node to proceed to the next group) shortens the logical distance to the destination, since node addresses should be strictly closer to the destination.

1.7 *PLGP Protocol with Vampire Attack*

In PLGP, the forwarding nodes do not know what path a packet took. This allows adversaries to divert packets to any part of the network, even if that area is logically further away from the destination than the malicious node. This makes PLGP vulnerable to Vampire attacks. Considering the directional antenna attack, a receiving honest node may be farther away from the packet destination than the malicious forwarding node, but the honest node has no way to tell that the packet it just received is moving away from the destination; the only information available to the honest node is its own address and the packet destination address, but not the address of the previous hop (who can lie). Thus, the Vampire can move a packet away from its destination without being detected. The situation is worse if the packet returns to the Vampire in the process of being forwarded—it can now be rerouted again, causing something similar to the carousel attack. Recalling that the damage from the carousel attack is bounded by the maximum length of the source route, but in PLGP the adversary faces no such limitation, so the packet can cycle indefinitely. Nodes may sacrifice some local storage to retain a record of recent packets to prevent this attack from being carried out repeatedly with the same packet. Random direction vectors, as suggested in PLGP, would likewise alleviate the problem of indefinite cycles by avoiding the same malicious node during the subsequent forwarding round.

1.8 *Modified PLGP*

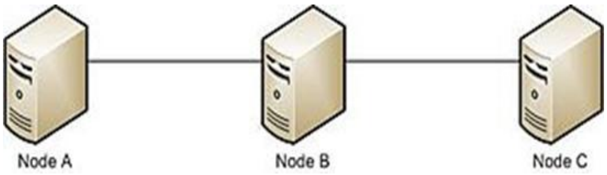
After having found that the original version of PLGP is vulnerable to vampire attacks, it was modified into PLGPa (PLGP with attestations) to resist vampire attacks during the packet forwarding phase. A property called the "no backtracking" property is introduced in this context. This property is satisfied for a given packet if and only if it consistently makes progress toward its destination in the logical network address space. No-backtracking implies Vampire resistance. The packet progress is checked independently where the nodes keep a record of route cost and communicate the local cost to the next hop. The next hop verifies if the remaining route cost is less than before and if the route cost is less then, the packet is progressing towards the destination and there is no malicious attack. This allows us to bound the attack in the network.

PLGP does not satisfy no-backtracking. PLGP differs from other protocols in that packets paths are further bounded by a tree, forwarding packets along the shortest route through the tree that is allowed by the physical topology. In other words, packet paths are constrained both by physical neighbour relationships and the routing tree. Since the tree implicitly mirrors the topology and every node holds an identical copy of the address tree, every node can verify the optimal next logical hop. However, this is not sufficient for no-backtracking to hold, since nodes cannot be certain of the path previously traversed by a packet. Communicating a local view of route cost is not as easy as it seems, since adversaries can always lie about their local metric, and so PLGP is still vulnerable to attacks, which allow adversaries to divert packets to any part of the network.

This PLGP was modified a little to preserve the property of no-backtracking. A verifiable path history was added to every PLGP packet. This resulted in PLGPa (PLGP with attestations). PLGPa uses this packet history together with PLGP's tree routing structure so every node can securely verify progress, preventing any significant adversarial influence on the path taken by any packet which traverses at least one honest node. Whenever node n forwards packet p, it does this by attaching a nonreplayable attestation (signature). These signatures form a chain attached to every packet, allowing any node receiving it to validate its path. Every forwarding node verifies the attestation chain to ensure that the packet has never traveled away from its destination in the logical address space. PLGPa satisfies no-backtracking.

II. DSDV PROTOCOL

Destination-Sequenced Distance-Vector Routing (DSDV) is a table-driven routing scheme for ad hoc mobile networks based on the Bellman–Ford algorithm. It was developed by C. Perkins and P. Bhagwat in 1994. The main contribution of the algorithm was to solve the routing loop problem. The above diagram shows a simple network with three nodes. Every mobile station maintains a routing table and each entry in the routing table contains all the available destinations, number of hops to reach the destination and sequence number assigned by the destination node. The sequence number is generally even if a link is present else it is odd and this sequence number is used to distinguish stale routes from new ones avoiding the formation of loops. The number is generated by the destination, and the emitter needs to send out the next update with this number.



The stations periodically transmit their routing tables to their immediate neighbours. A station also transmits its routing table if a significant change has occurred in its table from the last update sent. So, the update is both time-driven and event-driven. The routing table updates can be sent in two ways. One way is a "full dump" and the other is an incremental update. A full dump sends the full routing table to the neighbours and could span many packets whereas in an incremental update only those entries from the routing table are sent that has a metric change since the last update and it must fit in a packet. If there is space in the incremental update packet then those entries may be included whose sequence number has changed. When the network is relatively stable, incremental updates are sent to avoid extra traffic and full dump are relatively infrequent. In a fast-changing network, incremental packets can grow big so full dumps will be more frequent.

Each route update packet, in addition to the routing table information, also contains a unique sequence number assigned by the transmitter. The route with the highest (i.e. most recent) sequence number is used. If two routes have the same sequence number then the route with the best metric (i.e. shortest route) is used. Based on the past history, the stations estimate the settling time of routes. The stations delay the transmission of a routing update by settling time so as to eliminate those updates that would occur if a better route were found very soon. The only flaw is that DSDV requires a regular update of its routing tables, which uses up battery power and a small amount of bandwidth even when the network is idle and whenever the topology of the network changes, a new sequence number is necessary before the network re-converges.

III. ENHANCED DSDV PROTOCOL FOR TOPOLOGY DISCOVERY

PLGPa did bound vampire attack during the packet forwarding phase but the fact that it includes path attestations increases the packet size ,incurs penalties in bandwidth use and radio power too increases. And adding extra verification in the intermediate nodes also increases processor utilization, time and power. All this worthwhile when an adversary is present in the network else even an entirely normal network may run at a relatively low speed. While PLGPa is not vulnerable to Vampire attacks during the forwarding phase, it is not the same with the topology discovery phase and the bound to be placed during the discovery phase is still unknown. And moreover PLGPa can only resist the presence of adversaries when detected. They cannot prevent its occurrence completely.

In this paper, inputs from DSDV are taken and modified to make it an Enhanced DSDV protocol to provably secure the network topology discovery phase. The table-driven protocol is used in this context to provide secure topology discovery of the network. We discuss the three basic features of DSDV protocol. Since DSDV is table-driven, it requires regular update of its routing tables and this in turn uses the battery power and extra bandwidth even when the network is in an idle state. Next feature is that it is pro-active. DSDV doesn’t just respond but rather it controls the entire network. This may lead to slow convergence and slow propagation. And the third feature is that it is purely “anytime active” protocol. The last feature since its active all the time, it can use battery power and bandwidth for its own sake apart from the networks sake.

In an attempt to make the network more secure in the discovery phase, we have proposed modifications in DSDV protocol and implemented it using the ns-2 simulator to show the results. We have replaced the table system of DSDV with an index system which will not require frequent and regular updating of the status of the network. The updating process will take place only as and when required. This will help in cutting down the cost of battery and bandwidth usage. This makes DSDV from being pro-active to becoming on-demand. It does not have to manage the entire network as there will not be any table with regular updates. And lastly the protocol does not have to stay active all time and can be called by the sensor nodes only when there is a necessity for a connection establishment between the nodes. This makes it simple on the network which can be prevented from wastage of energy and bandwidth.

IV. CONCLUSION

In this paper, we have presented the stretch and carousel attacks with a model of randomly generated network topology and then we have briefed about the PLGP protocol by Parno, Luk, Gustad and Perrig, all of these defined by Eugene and Nicholas. This protocol bounds the damage caused during the packet forwarding phase. We then showed how an adversary can target not only packet forwarding phase but also route and topology discovery phases—if discovery messages are flooded, an adversary can, for the cost of a single packet, consume energy at every node in the network which has proved to be a drawback in the case of PLGP protocol. We have then come up with an enhanced DSDV protocol, which can possibly avoid the occurrence of vampire attacks during the discovery of the topology phase. We have showed the modifications done to the DSDV protocol via ns-2 simulator and have prevented vampire attacks from making its presence during the network topology discovery phase.

REFERENCES

[1] Eugene Y.Vasserman and Nicholas Hopper, Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks.

[2] Wikipedia.Destination sequenced distance vector (DSDV) protocol.

[3] Guoyou He, Networking Laboratory, Helsinki University of Technology, ghe@cc.hut.fi

[4] *Routing Protocols* for Ad Hoc Mobile Wireless Networks, Padmini Misra, misra@cse.wustl.edu

HOMOMORPHIC ENCRYPION METHOD IN CLOUD COMPUTING

Jetlin. C. P [#1,] P.anju[*2],k.priyadharshini[*3],R.induja[*4]

[#1,] Assistant Professor, Department of CSE, Karpaga Vinayaga college of Engineering & Technology, Maduranthagam.

[*2,*3,*4,] III CSE, Department of CSE, Karpaga Vinayaga college of Engineering & Technology, Maduranthagam.

anjuanjana795@gmail.com
Inducraziee@gmail.com

***Abstract* - Cloud computing plays a vital role in data storage, homomorphic encryption is one among the schemes of data storage with security. As the IT field is rapidly moving towards Cloud Computing, software industry's focus is shifting from developing applications for PCs to Data Centers and Clouds that enable millions of users to make use of software simultaneously.data storage can acheive through cloud but the securiry of datas cannot fulfilled by the cloud computing Now a new method, called fully homomorphic encryption was introduced(FHE) that performs computation with the encrypted data and send to the client and offers a realistic hope that such calculations can be performed securely in the cloud.**

***Keywords:* Cloud Computing, Homomorphic encryption, data storage**

I. INTRODUCTION

A cloud is a pool of virtualized computer resources. A cloud can: Host a variety of different workloads, including batch-style back-end jobs and interactive, user-facing applications • Allow workloads to be deployed and scaled-out quickly through the rapid provisioning of Virtual machines or physical machines • Support redundant, self-recovering, highly scalable programming models that allow Workloads to recover from many unavoidable hardware/software failures • Monitor resource use in real time to enable rebalancing of allocations when Cloud computing environments needed support grid computing by quickly providing physical and virtual Servers on which the grid applications can run. Cloud computing should not be confused with Grid computing. Clouds also support no *grid environments*, such as a three-tier Web architecture running standard Or Web 2.0 applications. A cloud is more than a collection of computer resources because a Cloud provides a mechanism to manage those resources. History The Cloud is a metaphor for the Internet, derived from its common depiction in network diagrams (or more generally components which are managed by others) as a cloud outline.

The underlying concept dates back to 1960 when John McCarthy opined that "computation may someday be organized as a public utility" (indeed it shares characteristics with service bureaus which date back to the 1960s) and the term The Cloud was already in commercial use around the turn of the 21st century. Cloud computing solutions had started to appear on the market, though most of the focus at this time was on Software as a service. 2007 saw increased activity, including Google, IBM and a number of universities embarking on a large scale cloud computing research project, around the time the term.

Cloud Computing already existed under different names like "outsourcing" and "server hosting.The development of homomorphic encryption provides yet another clear-cut approach to build SFE protocols. Informally, a homomorphic encryption scheme allows computation directly on encrypted data. It is clear that a SFE protocol can also be build quite straightforward using HE. Alice can now encrypt the input x and send the ciphertexts to Bob. Bob will compute f(x) directly on the ciphertext and send back the encrypted result that only Alice can decrypt. In this way, Bob will not be able to learn anything about x as long as the security of the homomorphic encryption scheme holds. Homomrphic properties of standard public key encryption schemes.A fully homomorphic encryption scheme E should have an efficient algorithm EvaluateE that, for any valid E key pair (sk; pk), any circuit C, and any cipher texts $\Psi i \leftarrow$ EncryptE (pk;mi) outputs

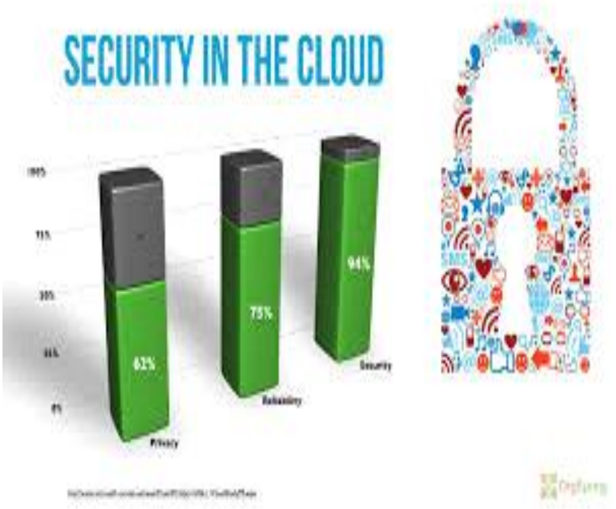
$\Psi \leftarrow$ EvaluateE (pk; C; $\Psi 1$ $\Psi 2$ $\Psi 3$……….. Ψt) such that
Decrypt E (sk;Ψ)=C(m1,m2,m3,…………………mt)

II. TECHNICAL SECURITY OF CLOUD COMPUTING

1. Centralized Data
2. Incident Response / Forensics
3. Password assurance testing (aka cracking)
4. Logging
5. Improve the state of security software (performance)
6. Secure builds
7. Security Testing

III.SECURITY ISSUES OF CLOUD

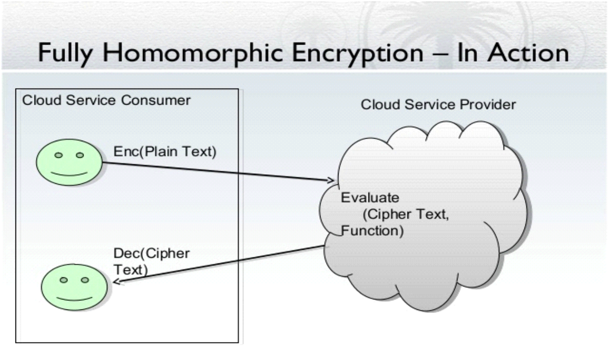
The definition of cloud computing that we mentioned in the previous section doesn't mention anysecurity notion of the data stored in the Cloud Computing even being a recent definition. Therefore we understand that the Cloud Computing is lacking security, confidentiality and visibility. To Provide Infrastructure (IaaS), Platform Service (PaaS) or Software (SaaS) as a Service is not sufficient if theCloud provider does not guaranty a better security and confidentiality of customer's data.By convention, we consider as Cloud Computing any treatment or storage of personal orprofessional information which are realized outside the concerned structure (i.e outside the company),to secure the Cloud means secure the treatments (calculations) andstorage (databases hosted by theCloud provider).Cloud providers such as IBM, Google and Amazon use the virtualization on their Cloud platform andon the same server can coexist a virtualized storage and treatment space that belong to concurrententerprises.The aspect of security and confidentiality must intervene to protect the data from each of theenterprises. Secure storage and treatment of data requires using a modern aspect of cryptography that energy reduction footprint of the company. e.g. RSA and ElGamal encryption, were recognized early on [7]. However they werelargely viewed as a weakness rather than an asset. Applications where data is statictypically require non-malleable encryption. However, the community has grown totrust the security of these schemes and, recently, the work of Gentry and othersdemonstrate that, when carefully employed, such homomorphic properties can bequite valuable. Indeed, a number of recent specific applications such as data aggregationin distributed networks, electronic voting, biometrics and privacy reserving data mining have led to reignited interest in homomorphic schemes.Many powerful HE schemes were proposed during the past decades.



1. *Homomorphic Encrpytion*

Homomorphic encryptions allow complex mathematical operations to be performed on encrypted data without compromising the encryption.When the data transferred to the Cloud we use standard encryption methods to secure this data, but when we want to do the calculations on data located on a remote server, it is necessary that the Cloud provider has access to the raw data, and then it will decrypt them. In this paper we propose the application of a method to perform the operation on encrypted data without decrypted and provide the same result as well that the calculations were carried out on raw data.n. The client will need to provide the private key to the server (Cloud provider) to decrypt data before execute the calculations required, which might affect the confidentiality and privacy of data stored in the Cloud.

5.



2. *Pratial Homomorphic Schemes*

It is clear that one of the most important goals of the researches about the homomorphic encryption schemes is to make them closer to practical applications. In this section, we will discuss possible ways to achieve it. Before we can even discuss thepractical HE schemes, we need to define the criteria for a scheme to be considered practical.The first requirement we set is versatility of the scheme, i.e., the scheme shouldsupport a large range circuits. This is the feature that most partial HE schemes are missing. It is easy to see that FHE schemes are extremely powerful in terms of versatility. However, fully homomorphism is not a necessary. The BGV and LTV schemes give perfect example of this. Both schemes can perform recryption and achieve fully homomorphism, however, in most cases, the recryption is left asan optimization. In [30], the full AES rounds are evaluated using the BGV schemewithout recryption. In other words, the BGV scheme is used as a partial HE schemeor Somewhat HE scheme instead of a “Fully” HE scheme in this case. In conclusion,the versatility is an important requirement for a HE scheme to be practical. As wediscussed in previous sections, it is the low efficiency that stops existing FHE schemesfrom being employed in practical applications. In detail, neither the efficiency in terms of computation or cipher size is satisfactory. Since the reduce the ciphertext size are quite different, we separate them into two categories. Hence, there are three basic approaches to improve the computation speed and to requirements:

3. *PRATICAL SCHEMES*

- Versatility
- Speed
- Ciphertext Size

4. *Challenge Of Homomorphic Encryption:*

The homomorphic properties of various encryption schemes were recognized in 1978 by Rivest,Adleman, and Dertouzos in [RAD78]. Theypublished a paper proposing the use of ‘privacy homomorphisms’ to not only secure data, butallow it to be used by untrusted parties. Rivest and Adleman, two of the three cryptographersbehind the popular RSA encryption scheme, would later go on to found the RSA security firm in 1982 Consider a small loan company which uses a commercial time-sharing service to store its records. The loan company’s ‘data bank’ obviously contains sensitive information which should be kept private. On the other hand, suppose that the information protection techniques employed by the time sharing service are not considered adequate by the loan company.

5. *Recent Advances In Homomorphic Encryption*

Traditionally, data confidentiality is a matter of cryptographers and is addressed through the design and use of encryption schemes. But while there is a permanent need of common encryption methods like RSA or the Advanced Encryption Standard(AES), interest in specific schemes has grown and spread during the last 30 years to more and more fields, encompassing signal processing. This is most notably due to the deployment of multimedia content distribution platforms, the development of biometric techniques, and the widespread adoption of the cloud computing model for more and more critical applications.In such applications, some parties (often end users) may want to preserve the privacy of the data they outsource, or of their requests to servers. As a straightforward example, an enduser might want to preserve the confidentiality of his e-mails

IV.IBM's HOMOMORPHIC ENCRYPTION COULD REVOLUTIONISED SECURITY

IBM gets a patent on an encryption method that could make it possible to run fully encrypted programs or VMs without first decrypting them.IBM has been granted a patent on an encryption method that, if implemented, could be revolutionary. It makes it possible to process encrypted data without having to decrypt that data first.Internet of things Deep Dive The Internet of things: What it is, where it's going The Internet of things is a big, confusing field waiting to explode. Get the scoop on this read now Known as "fully homomorphic encryption," this encryption method has long been something of a Holy Grail for computer scientists, and IBM in particular has been seeking this particular prize for years.

V. FUTURE PLANS

As cloud computing is a large area and use of cloud computing is increasing daily. Again cloud having 3 service model that are software as a service (saas), platform as a service (paas), and infrastructure as a service(iaas) so everyone is looking to move into the cloud as it give more flexibility and reduced cost. Here we haveimplement fully homomorphic encryption scheme where all type of operation are can be performed without knowing secret key. The main defect of this scheme is that after encrypt the size of data become very large which will cause heavy burden for network and storage.

VI. CONCLUSION

The Security of Cloud Computing based on fully Homomorphic Encryption is a new concept ofsecurity which is enable to provide the results of calculations on encrypted data without knowing the raw entries on which the calculation was carried out respecting the confidentiality of data.In future, we are going to analyse the behaviour of Homomorphic Encryption cryptosystems compared to the length of the public key and the time of the treatment of the request by the Cloud provider depending on the size of the encrypted message Skepticism about the most recent set of breakthroughs remains strong, however. Bob Gourley of CTOvision.com writes, "I have seen nothing in any of the research that makes me think a solution can be put in place that cannot be defeated by bad guys. And if that can’t be done then the solution will not solve any problems, it will just add processing overhead."In other words, the biggest problems may not lie with HIM itself, but rather with how well it's implemented -- a common weakness with encryption technology in general. While still being able to set up filters or to perform searches.

REFERENCES

[1] [Sean] Marston and al. “Cloud computing — The business perspective”, Volume 51, Issue 1, Pages176–189, http://www.sciencedirect.com, April 2011.

[2] Creepy puppet, “A Survey of Virtualization Techniques in Cloud Computing”, Proceedings ofInternational Conference on VLSI, Communication, Advanced Devices, Signals & Systems andNetworking (VCASAN-2013), Volume258, 2013, pp 461-470, springer, 2013.

[3] Vic (J.R.) Winkler, “Securing the Cloud, Cloud Computer Security, Techniques and Tactics”,Elsevier, 2011.

IMAGE SEGMENTATION BASED ON PSO: A SURVEY OVER ALGORITHMS

Adeelah DG#1, R.Rajeswari*2

** M.Phil. Research Scholar, Department Of Computer Applications, Bharathiar University, Coimbatore, Tamilnadu.*
# Assistant Professor, Department Of Computer Applications, Bharathiar University, Coimbatore, Tamilnadu.

adeesana@gmail.com
rrajeswari@rediffmail.com

***Abstract*-- Image segmentation, which is the process of segmenting the image into regions which have similar features, is one of the important tasks in image processing. Various bio-inspired algorithms have been used for image segmentation. Recently, particle swarm optimization (PSO) is used in image segmentation. This paper gives a review of different algorithms proposed for image segmentation using PSO. This study will be helpful for an appropriate use of existing methods in segmentation using PSO.**

***Keywords*—segmentarion; PSO; Various algorithms Of PSO**

I. INTRODUCTION

Image segmentation is one of the important tasks in image processing and computer vision. It is a process of segmenting whole input image into several regions based on similarities and differences that is presented in the pixels of that input image.[1].The goal of image segmentation is to get meaningful objects from the input images. Most computer vision and image analysis problems require a segmentation stage in order to detect objects or divide the image into regions. Image segmentation is used in several applications including video surveillance, medical imaging analysis, image retrieval and object classification [2].

Particle Swarm Optimization (PSO) was developed by James Kennedy and Russell C Eberhart in 1995 [3]. PSO belongs to the class of swarm intelligence techniques that are used to solve optimization problems. PSO is a population-based stochastic approach for solving continuous and discrete optimization problems based on the movement and intelligence of swarms. In particle swarm optimization, number of agents, called particles, move in the search space of an optimization problem. The position of a particle represents a candidate solution to the optimization problem. Each particle searches for better positions in the search space by changing its velocity according to rules originally inspired by behavioral models of bird flocking [4].

Each particle's movement is influenced by its local best known position but, is also guided toward the best known positions in the search-space, which are updated as better positions found by other particles. This is expected to move the swarm toward the best solutions. The basic concept of the algorithm is to create a swarm of particles which move in the space around them (the problem space) searching for their goal, the place which best suits their needs given by a fitness function. A nature analogy with birds is the following: a bird flock flies in its environment looking for the best place to rest (the best place can be a combination of characteristics like space for all the flock, food access, water access or any other relevant characteristic) [5]. The PSO based segmented images are generally well segmented into regions of homogeneous colour and are perceptually meaningful to human's vision. This paper gives a review of recent work in image segmentation using particle swarm optimization. The rest of this paper is organized as follows, Section II gives an overview of the recent work in image segmentation using PSO and Section III concludes the paper.

II. LITERATURE SURVEY

Gao et al [6] developed a new algorithm called intermediate disturbance PSO (IDPSO), which intensifies the global search ability of particles and increases their convergence rates. The objective was to employ the proposed strategy to not only accelerate convergence speed but also to avoid the local optima of PSO. The experimental results after comparing the IDPSO to ten known PSO variants on 16 benchmark problems demonstrated the potency of the proposed algorithm. IDPSO algorithm was also applied to multilevel image segmentation problem for shortening the computational time. The results obtained from the experiments of new algorithm on a variety of images showed that it can effectively segment an image faster.

Li a et al [7] introduced an algorithm called Dynamic Context Cooperative Quantum-behaved particle swarm optimization (CCQPSO). The aim of this algorithm was to improve performance of the cooperative quantum-behaved particle swarm optimization (CQPSO) algorithm by just utilizing its context information. It was also shown that CCQPSO algorithm can be used in Otsu image segmentation to optimize the parameters and they have applied this method for a number of medical image

Chander et al [8] introduced an algorithm for optimal multilevel threshold. It uses an iterative scheme to obtain initial thresholds. This new algorithm is more suitable compared to other well-known methods if there is any exponential growth in computing complexity. A new contribution in adapting 'social' and 'momentum' components of the velocity equation for PSO updates is also made. Experiments performed on four well known images such as Lena, pepper, elaine and house. This shows that that new algorithm produced better result compared to other methods.

Deren et al [9] introduced particle swarm optimization into fuzzy entropy image segmentation for selecting the optimal fuzzy parameter combination and fuzzy threshold adaptively. The segmentation experiments are done by using remote sensing images such as IKONOS and Landsat-5 TM. The PSO method obtained the same optimal fuzzy parameter combination and fuzzy threshold as that of the exhaustive search while its search time is less than that of the exhaustive search when applied to different kinds of remote sensing images. The Proposed PSO based method had good search stability in all experiments.

Mahamed et al [10] introduced a new dynamic clustering algorithm based on PSO with application to image segmentation known as Dynamic clustering using particle swarm optimization (DCPSO) algorithm. This approach automatically finds out the optimum number of clusters and at the same instance it clusters the data set with lesser user interference. One of the advantages of this algorithm is that it can work with any validity index. The DCPSO algorithm uses the K-means clustering algorithm to refine the cluster centroids. The experiment was done on synthetic as well as natural images and result proved that the proposed approach found the optimum number of clusters on the tested images.

Liu et al [11] developed a modified particle swarm optimization (MPSO) algorithm .This algorithm was presented in the field of image segmentation for solving multilevel thresholding problem. The MPSO uses two new strategies to improve the performance of original particle swarm optimization (PSO), which are named as adaptive inertia (AI) and adaptive population (AP). The MPSO was applied for solving multilevel thresholding problems of 16 standard test images based on the Otsu's method, and it is compared with the global PSO (GPSO) and standard genetic algorithm (SGA) to validate its performance. The experimental results show that MPSO improves the performance of the PSO model. The MPSO was also used to find the optimal thresholds by maximizing the Otsu's objective function and its performance have been validated on 16 standard test images. The experimental results of 30 independent runs illustrate the better solution quality of MPSO when compared with the global particle swarm optimization and standard genetic algorithm

Manikantana et al[12] Introduced Golden Ratio Particle Swarm Optimization (GRPSO)-.It is based on Golden Ratio found in nature. This algorithm was used for determining optimal thresholds for improved image segmentation. GRPSO algorithm is used to perform multilevel thresholding based on objective function Tsallis entropy method. Objective values achieved by GRPSO had been compared with those achieved by Genetic Algorithms (GA), Particle Swarm Optimization (PSO) and BF for 5 standard grey level images. It is clear from experimental results that GRPSO achieves higher objective values which results in improved image segmentation.

Lee et al [13] proposed a saliency directed colour image segmentation approach using particle swarm optimization. In this approach both low-level features and high-level image semantics extracted from each colour image are utilized. To extract high-level image semantics from each colour image, the visual attention saliency map for each colour image is generated by three (colour, intensity, and orientation) feature maps, which is used to guide region merging using 'simple' modified particle swarm optimization (PSO).The proposed approach contains four stages, namely, colour quantization, feature extraction, small region elimination, and region merging using a modified PSO. Experimental results shows that after comparing it with four different approaches like Otsu thresholding (Otsu) ,dynamic clustering using PSO (DCPSO), the mean-shift approach (MeanShift), and the binary partition tree approach(BPT) , the proposed approach provides better colour image segmentation result.

Feng et al [14] have applied Particle swarm optimization (PSO) and 2-D maximum entropy based image segmentation to infrared images and found that it was a simple and very effective method. It is very much helpful in the system where real time processing is needed. The experiments of segmenting the infrared images show that the proposed method can get ideal segmentation result with less computation cost.

Fahd et al [*15]* paper presents a new image segmentation method called PSO-Seeded Region Growing (SRG).It is developed by combining PSO algorithm

III. CONCLUSION

This paper presents a summary of image segmentation based on particle swarm optimization (PSO). It highlights many algorithms in which PSO was successfully applied for image segmentation. This review will be useful for an appropriate use of existing methods in segmentation using PSO.

REFERENCES

[1] H. Shah-Hosseini, "Multilevel Thresholding for Image Segmentation using the Galaxy-based Search Algorithm," *Int. J. Intell. Syst. Appl.*, vol. 5, no. October, pp. 19–33, 2013.

[2] Y. Zhang, D. Huang, M. Ji, and F. Xie, "Expert Systems with Applications Image segmentation using PSO and PCM with Mahalanobis distance," *Expert Syst. Appl.*, vol. 38, no. 7, pp. 9036–9040, 2011.

[3] A. A. Esmin and G. Lambert-Torres, "Application of particle swarm optimization to optimal power systems," *Int J Innov Comput Inf Control*, vol. 8, no. 3, pp. 1705–1716, 2012.

[4] F. Mohsen, M. Hadhoud, K. Mostafa, and K. Amin, "A New Image Segmentation Method Based on Particle Swarm Optimization," *Int. Arab J. Inf. Technol.*, vol. 9, no. 5, pp. 487–493, 2012.

[5] J. Kennedy and R. Eberhart, "Particle swarm optimization," *Proc. ICNN'95 - Int. Conf. Neural Networks*, vol. 4, 1995.

[6] H. Gao, S. Kwong, J. Yang, and J. Cao, "Particle swarm optimization based on intermediate disturbance strategy algorithm and its application in multi-threshold image segmentation," *Inf. Sci. (Ny).*, vol. 250, pp. 82–112, 2013.

[7] Y. Li, L. Jiao, R. Shang, and R. Stolkin, "Dynamic-context cooperative quantum-behaved particle swarm optimization based on multilevel thresholding applied to medical image segmentation," *Inf. Sci. (Ny).*, vol. 294, pp. 408–422, 2015.

[8] A. Chander, A. Chatterjee, and P. Siarry, "A new social and momentum component adaptive PSO algorithm for image segmentation," *Expert Syst. Appl.*, vol. 38, no. 5, pp. 4998–5004, 2011.

[9] L. Li and D. Li, "Fuzzy entropy image segmentation based on particle swarm optimization," *Prog. Nat. Sci.*, vol. 18, pp. 1167–1171, 2008.

[10] M. G. H. Omran, A. Salman, and A. P. Engelbrecht, "Dynamic clustering using particle swarm optimization with application in image segmentation," *Pattern Anal. Appl.*, vol. 8, pp. 332–344, 2006.

[11] Y. Liu, C. Mu, W. Kou, and J. Liu, "Modified particle swarm optimization-based multilevel thresholding for image segmentation," *Soft Comput.*, 2014.

[12] K. Manikantan, B. V. Arun, and D. K. S. Yaradoni, "Optimal multilevel thresholds based on Tsallis Entropy method using golden ratio particle swarm optimization for improved image segmentation," *Procedia Eng.*, vol. 30, no. 2011, pp. 364–371, 2012.

[13] C.-Y. Lee, J.-J. Leou, and H.-H. Hsiao, "Saliency-directed color image segmentation using modified particle swarm optimization," *Signal Processing*, vol. 92, no. 1, pp. 1–18, 2012.

[14] D. Feng, S. Wenkang, C. Liangzhou, D. Yong, and Z. Zhenfu, "Infrared image segmentation with 2-D maximum entropy
method based on particle swarm optimization (PSO)," *Pattern Recognit. Lett.*, vol. 26, pp. 597–603, 2005.

SMART HOUSE FOR AGED

D.NANDHINI [#1], C. SHRIDEVI [*2]

[#] *Panimalar Engineering College, Chennai*
[*] *Panimalar Engineering College, Chennai*

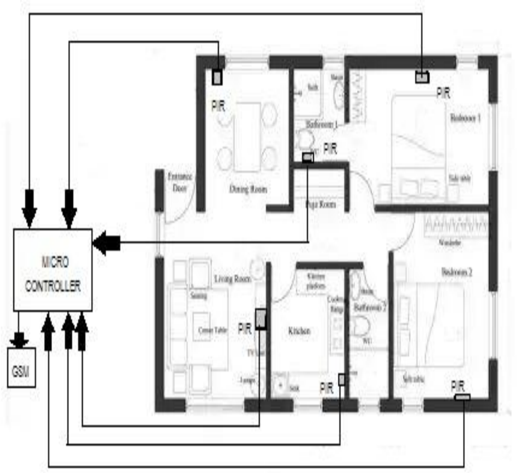
***Abstract*-Security is a critical issue in case of elderly people in homes. In this proposal, we are proposing a device which helps in monitoring the elderly people. This device keeps on checking the activities of the person every five minutes using a special type of sensor like PIR sensor which senses every activity, collect them and stores it. These data are stored in microcontroller and the activities of them can be monitored by the care taker by means of GSM technology. In this, all the activities are monitored but only the major activities like walking, sitting etc. are taken into account while other minor activities like turning of a person head, hands etc. are ignored. The benefit of this device is that the elder person privacy is secured because there is no usage of CCTV cameras and they are not equipped with any kind of instruments.**

***Keywords*-Monitoring of the elderly people, major activities like walking, sitting action etc., PIR sensors, microcontroller, and GSM technology**

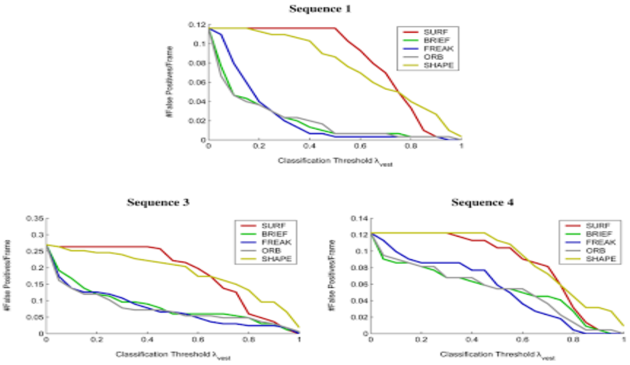
I. INTRODUCTION

Today we are living in the 21st century where the smartness in technology is highly in demand. Due to the advancement of the wirelesstechnologies, there are several different connections are being . introduced, which has its own unique specifications and applicationThe security and the emergency system for the aged people were only accessed only through the Bluetooth by the doctors and their caretakers. Since bluetooth can over only a limited range, it becomes a drawback of it. GSM has been introduced which can provide high efficiency & reliability for monitoring the aged people for sick by accessing them through web. The aged people are monitored when needed through this technology. GSM can operate in the frequency range of 900-1800 MHz . So it ensures security and overall protection at its best with the help of its implementation in ATMEL AT Mega 168PB X-plained mini kit. If any unusual activity is encountered, then the system will send the alert the respective person

II. PROPOSED ARCHITECTURE



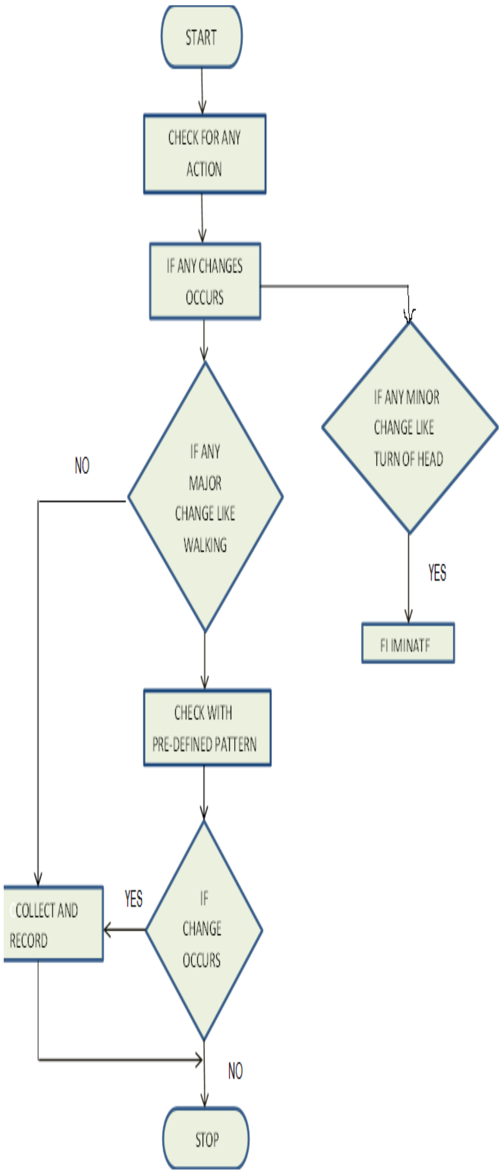
III. WORKING PRINCIPLE



Like most of the machine learning systems, movement of the system needs to be monitored. Here the movement is extracted or monitor using special type of sensors called of PIR sensor. Using this PIR sensor, each and every activity of the persons are noted. And it is differentiated from the usual reflex that has been programmed. These activity details are collected differentiated and stored in a microcontroller where it is programmed using a ATMEL AT Mega 168PB X-plained software. The person activity is monitored for every 5 seconds and compared with the designed pattern. If there are any variations in the recordings, then it is updated and it is alerted to the caretaker through GSM technology. The major activates like walking, sitting, turning around etc., are taken into account while minor activities like movement of the curtain, turning of head are ignored. Thus by this method, the daily activates of the elderly person at home is monitored and the health issues are taken into account and the security is maintained. The elderly persons are not burdened with any kind of equipment by this method. The privacy of the elderly is not violated because there is no usage of CCTV cameras.

Fig1. Movement monitored by the sensor

IV. CONCLUSION



The work presented above assures utmost security and satisfies the thirst for the smart technology especially for elderly people who take care of them. These systems are totally safe from any harm and are reliable over longer span. As the data are being daily updated they can be reviewed for future clarifications.

REFERENCES

[1] S. Lanspery and J. Hyde, “Introduction: Staying put”, In Lanspery S, and Hyde J Staying put: Adapting the places instead of the People, Amityville, NY: Baywood Publishing, **(1997)**, pp. 1-22.

[2] E. Dishman, “Inventing Wellness System for Aging in Place”, IEEE Computer Magazine, vol. 37, no. 5, **(2004)**, pp. 34-41.

[3] S. Stowe and S. Harding, “Technology applied to geriatric medicine: Telecare, telehealth and telemedicine”, European Geriatric Medicine, vol. 1, **(2010)**, pp. 193-197.

[4] P. Klasnja and W. Pratt “Healthcare in the pocket: Mapping the space of mobile-phone health interventions”, Journal of Biomedical Informatics, vol. 45, **(2012)**, pp. 184–198.

[5] P. Kulkarni and Y. Ozturk, “mPHASiS: Mobile patient healthcare and sensor information system”, Journal of Network and Computer Applications, vol. 34, **(2011)**, pp. 402-417.

EMERGENCY APP USING REAL TIME GPS TRACKING

Akshay Moorthy[#1], Mary Joseph[*2]

[#] *UG Student Department of CSE, Anand Institute of Higher Technology, Chennai*
[*] *Assistant Professor Department of CSE, Anand Institute of Higher Technology, Chennai*

m.akshay9@gmail.com

***Abstract* - Personal safety in India has become an issue of importance for everyone, especially for women. The advancement in recent technologies can have a huge impact in reducing crime rates. In this paper, an idea has been proposed to create an Android application that uses the GPS to find people nearby. It allows them to track the user, using real time GPS tracking. At the same time it alerts the Police to provide assistance for any Smartphone user, while in danger.**

***Keywords* - GPS, Android, Tracking.**

I. INTRODUCTION

In this modern era, advancement in mobile technologies has led the Smartphone's to become part and parcel of human beings as they are used extensively. Smartphone's have changed our way of living due to advanced functionalities that the mobile OS can provide.In India, due to increased crime rates people feel insecure when they move out and when they are in a danger it becomes practically impossible to reach out for help. In this paper, an idea has been proposed to create an Android app that can reach people within the vicinity.

The introduction of mobile computing has redefined the way of human-computer interaction. It provides decentralized computations on diversified devices, systems, and networks, which are mobile, synchronized, and interconnected via mobile. The Global Positioning System (GPS) is a worldwide radio-navigation system formed from a constellation of 24 satellites and their ground stations. GPS uses these "man-made stars" as reference points to calculate positions accurate to a matter of meters. In fact, with advanced forms of GPS we can make accurate measurements to a matter of centimeter.

II. LITERATURE REVIEW

There are some applications [2] that marks the nearby location using GPS and sends the message to the family members whose numbers are saved in the database Some of the disadvantages with these apps is that every time to send the messages we have to unlock the mobile and then double tap on the app icon. Sometimes it may happen that a person may unknowingly tap on the app for multiple times and false message will be sent to the members in the database.

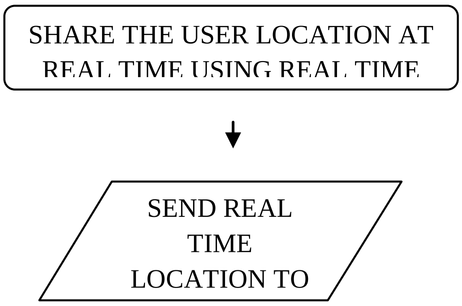
Papers have been proposed to develop an emergency app using voice recognition [1].The idea uses voice recognition concept to match and accept user's voice as input and send location details to the number stored in database. The major disadvantage of this app is that, it can't be used in a noisy surroundings and also that the probability of voice mismatch is high. Papers have also been proposed to implement tri-axial accelerometer as a trigger to send location [3]. The major disadvantage of this technique is that mishandling of device can also trigger the event unnecessarily.

The recognition failure, voice mismatch and time delays during emergency situation may lead to grave consequences. So, I have suggested an idea that can overcome these disadvantages by incorporating the real time GPS tracking in the emergency app. This will work in the way that without unlocking the mobile and without tapping on the app icon we are able to establish connection to people and authorities nearby by pressing the configured emergency button. Instead of having this application as a secondary choice, I insist to embed this app along with the OS so as to provide this functionality for every Smartphone user and to provide ease in assistance.

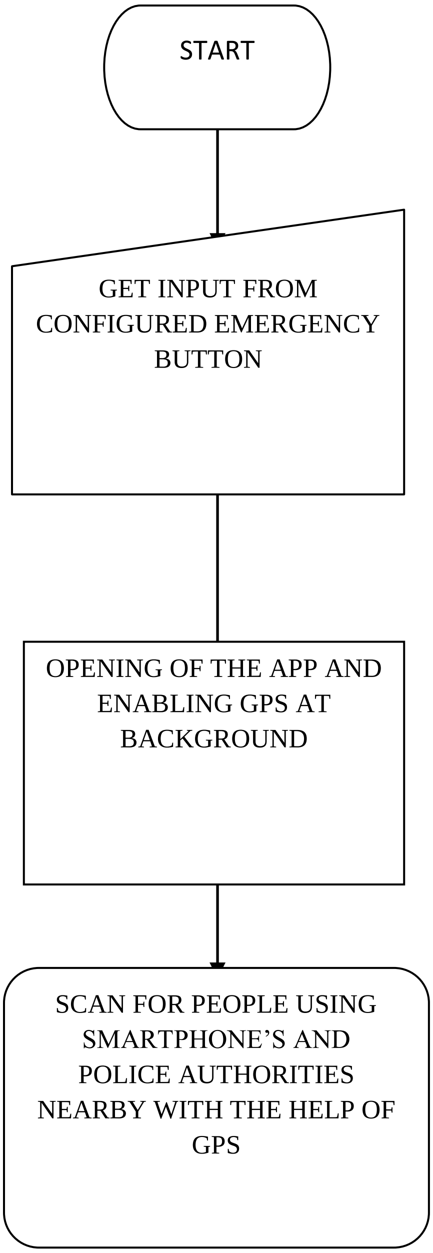
III. METHODOLOGY

The process of my proposed Android application would start when the user presses the configured emergency button. Then at the background the application starts to search for people using Smartphone's and the authorities nearby with the help of GPS and shares the location with them after which it allows the people to track the user in real time using Real Time GPS Tracking.

User End


SHARE THE USER LOCATION AT REAL TIME USING REAL TIME
SEND REAL TIME LOCATION TO

Receiving End


START
GET INPUT FROM CONFIGURED EMERGENCY BUTTON
OPENING OF THE APP AND ENABLING GPS AT BACKGROUND
SCAN FOR PEOPLE USING SMARTPHONE'S AND POLICE AUTHORITIES NEARBY WITH THE HELP OF GPS

IV. GRAPHICAL REPRESENTATION

Stage 1:

During emergency, the victim presses the configured emergency button in order to communicate with people nearby as shown in Fig.1

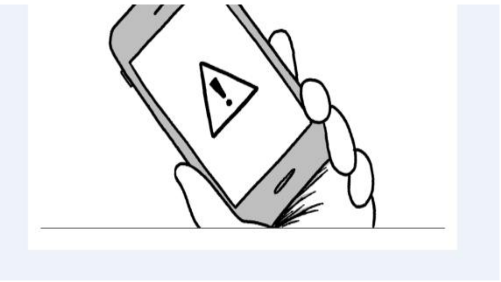
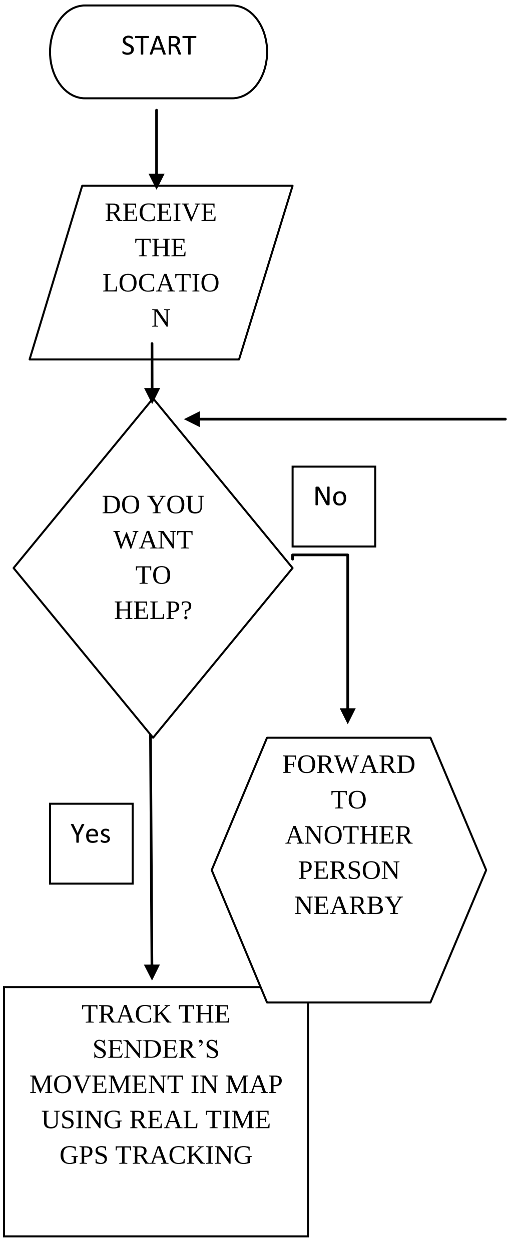


Fig.1Stage 2:

As soon as the button is pressed, the app opens up at background and starts scanning for people and police authorities with Smartphone in the vicinity as shown in Fig.2


START
RECEIVE THE LOCATIO N
DO YOU WANT TO HELP?
No
FORWARD TO ANOTHER PERSON NEARBY
Yes
TRACK THE SENDER'S MOVEMENT IN MAP USING REAL TIME GPS TRACKING

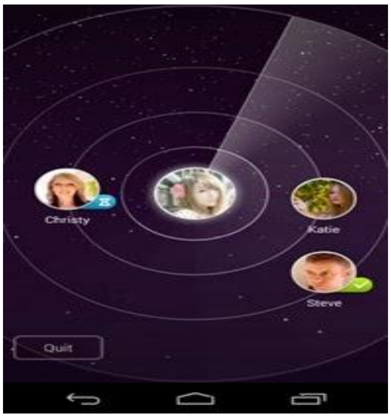


Fig.2

Stage 3:

After scanning it sends “help” message to them and asks for receiver’s decision whether to help or not as shown in Fig 3.

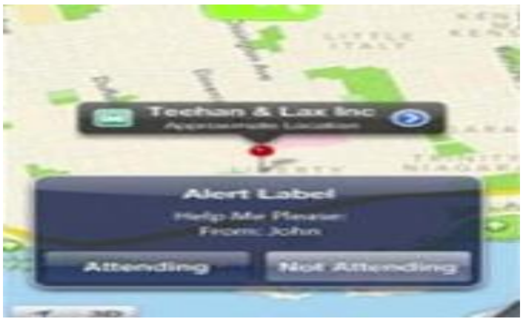

Techan & Lax Inc
Approximate Location
Alert Label
Help Me Please
From: John

Fig 3.

Stage 4: If the receiver accepts to help then the victims location gets shared in real time using Real Time GPS tracking else the receiver can either reject or forward the message.Tracking of the victim in real time is as shown in Fig.4.

Example:

Consider a man returning home after work at evening. Suddenly a bandit blocks him and tries to stab him in order to steal the victim’s belongings. At this time if the victim presses the emergency button in his Smartphone, the app would open automatically and find the people and authority nearby using GPS and share the location of victim. If the receiver’s receiving the message agree to help, then they can have a real time track on the victim and follow them throughout or even call out for help using the Real Time GPS Tracker. In a case where the receiver doesn’t wish to help, he can forward the location to someone else nearby.

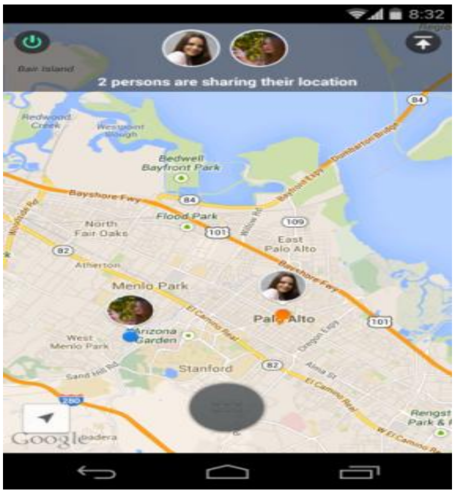

2 persons are sharing their location

Fig 4.

V.CONCLUSION

Thus the idea of creating such an app can reduce crime rates and provide protection to people, especially for women. It may also help the police authorities to keep a track on victim till they arrive and can also help seek interim and immediate assistance from people nearby. If my idea of implementing real time GPS tracking in emergency app succeeds then I have planned to add few more features such as one touch fingerprint authentication instead of emergency buttons in order to avoid misuse and also auditory emotions to automatically detect danger situations using victims voice as audio signals. Usage of technology for ensuring ones safety by developing such apps can build a safer and crime free nation thereby protecting people.

REFERENCES

[1] P.Tejas, W.Sonali, C.Vaishali, “Emergency App using Voice Recognition” IJCAT International Journal of Computing and Technology, Volume 1, Issue 2, March 2014

[2] STAR India Pvt. Ltd, “VithU” Android Application, Google Play Store

[3] “Emergency Application for Women” IJSRP Volume 4 Issue 3 March 204

ONLINE VOTING THROUGH SMARTPHONES IMPLEMENTATION USING MOBILE COMPUTING

B.Monisha [#1], S.Abirami[*2], S.Gayathri priyadharshini[*3] and Prasanth Yokesh[*4]

[#1]*Anand Institute of Higher Technology, Chennai*
[*2]*Anand Institute of Higher Technology, Chennai*
[*3]*Anand Institute of Higher Technology, Chennai*
[*4] *Assistant professor, Anand Institute of Higher Technology, Chennai*

***Abstract*—Mobile computing is an emerging concept combining the many fields of computing. The objective is to set up a online voting through smartphones. The advancement in the mobile devices, wireless and web technologies given rise to the new application that will make the voting process very easy and efficient. The online-voting promises the possibility of convenient, easy and safe way to capture and count the votes in an election. This research project provides the specification and requirements for online voting using an Android platform. The android platform is used to develop an online voting application. The scope of the project includes testing and analyzing the performance of applications in the scientific and engineering domain on the installed mobile infrastructure.**

***Keywords*- Online voting, Short Message Service(SMS),UniversalTelecommunications System (UMTS), Quick Response Code (QR Code).**

I. INTRODUCTION

The proper execution of democratic rights has become linked to the availability and reliable functioning of advanced information and communication technology (ICT). While modern societies fully rely on ICT for business, work and leisure time activities, the use of ICT for democratic decision making is still in its infancy. In fact, the out date technological concepts for voting have been blamed in part for lost and uncounted votes and could therefore be responsible for biased political decisions making. Countries all over the world are examining online voting, for it has some striking advantages over traditional paper voting, including security for centralized and decentralized manner, etc.

Mostly in an inherent lack of trust and fear of electronic threats. While most countries are still conceptualizing or testing online voting systems, three cantons in Switzerland have pioneered the development of online voting to its full technological maturity. The world is always in improvement and growth in technology, that's why we should go parallel with it, to be able as much as we can get benefit from these improvements.

Via SMS: each voter can vote by sending an SMS using any kind of mobile connection line or any kind of mobile hand set to the system through the "Mobile Switch Center". For this such type system, an android application is created in Android phone, then the system will start implementing some processes on that SMS which is sent by the voters into the server through a network. A (MySQL) database is installed on the server side to send a result back to the voter by the android system application.Both Android system and the Website are linked to the (MySQL) database in order to the voter can vote through one of the two ways only one time and if he/she tries to vote again the system will deny him/her.

II. ONLINE VOTING SYSTEM SURVEYS

Android Online Voting application on smart phone user gives user to vote, an application with an interface for consultation to a dynamic web page offers the main question to be answered (voted), and together to this page are available the buttons to send the votes: Yes, No or Maybe. Admin can see the voting results according to vote options and country from which vote was done and also can see the location of particular voter using GPS. The User can submit his opinion about given topic. System can maintain the data about the voter like Name, Country, ID number and opinion about given topic.

Even though the system enables voters to poll their vote from anywhere, initially the voters should have to provide their voter id number to authenticate themselves and establish their user-ids. This constraint is imposed to ensure that only the genuine person is allowed to vote in the elections. The aim of this work is to design and implement an electronic voting application for the Android platform that will enable people to vote securely from anywhere. The application as a whole is aimed at being compatible with devices from many manufacturers and running different versions of the operating system. The application is also aimed at being localized.

Online voting refers to the use of computers or computerized voting equipment to cast ballots in an election. Sometimes, this term is used more specifically to refer to voting that takes place over the Internet. Electronic systems can be used to register voters, tally ballots, and record votes.

The NSF Internet Voting Report addresses the feasibility of different forms of Internet voting from both the technical and social science perspectives, and defines a research agenda to pursue if Internet voting is to be viable in the future. It groups Internet voting systems into three general categories as follows:

- Poll-site Internet voting: It offers the promise of greater convenience and efficiency in that voters could cast their ballots from any poll site, and the tallying process would be both fast and certain. More importantly, since election officials would control both the voting platform and the physical environment, managing the security risks of such systems is feasible.
- Remote Internet voting: It seeks to maximize the convenience and access of the voters by enabling them to cast ballots from virtually any location that is Internet accessible. While this concept is attractive and offers significant benefits,

it also poses substantial security risks and other concerns relative to civic culture. Current and near-term technologies are inadequate to address these risks.

The report presents some findings on the feasibility of each of these categories and provides research recommendations for the long-term future. It then identifies criteria for election systems. Finally, it addresses the technological issues (including voting system vulnerabilities, reliability, testing, certification and standards, specifications of source code, platform compatibility, secrecy and non-coercibility, etc.) and social science issues (such as voter participation, voter access, the election process, voter information, deliberative and representative democracy, community and character of elections, distribution of roles, legal concerns, voter registration, etc.)

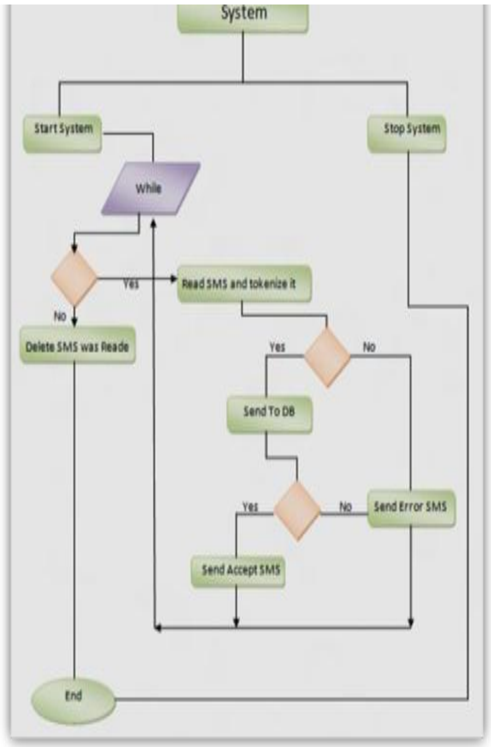
This project investigates broadband mobile communications based on the UMTS standard for providing the network with the required bandwidth and security. This makes it possible to use anywhere, within a private, reliable and protected network. The voter-recognition system is based on an innovative smart card with an embedded biometric fingerprint reader, which performs voter recognition with absolute security. An ergonomic kiosk facilitates use by disabled people.

III. ONLINE VOTING SYSTEM DESIGN

Like most of the systems in the world, the security consideration is very important. We are taken into account this part through the limitation of the access using face recognition technique. When we click on a program icon , the system asks for a face to recognize ,when the system recognizes the face of the (Admin) it will gives him the approval to access the system, if the system couldn't recognize the face under any conditions for example : not clear face, too much light , the system will ask for password as an additional option. If the Admin could not access the system because of the above conditions, the system will deny him for access and the Admin will try again from the face recognition step. Also another technology that is used in this system is by using Hand Gesture Recognition in order to control all Tabs without touching the screen of the smart phone. This technique is successfully applied by using (Proximity sensor), that located in the upper layer of the android phone.

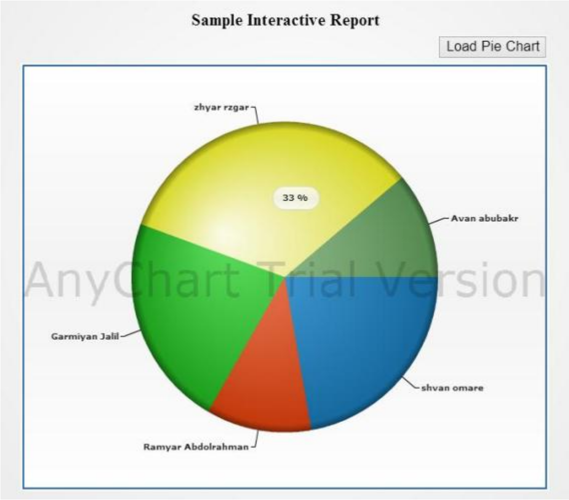
A. ***The first way for Voting(SMS Voting) :*** The voter can vote through the mobile regardless of the type by sending SMS to the system which are contains the following information.

After the system receiving the SMS from the voters, the SMS will go to the Inbox part of the phone. Then, the system will find the SMS and save the header information. The system will separate SMS information and tokenizes them into several parts in order to work on them. The System will check those parts in order to know if they were sent in the right way that the system specified earlier, if there was an error in the information of SMS the system will send the SMS to the voter to tell him/her that the SMS contains wrong information. If the SMS did not have any errors, the information will be sent by the network to the server. The server double checks the SMS information to make sure the voter did not vote before. If the voter did not vote before, the server will accept the vote and the system sends an SMS to the voter that the vote has been accepted. After that the system will delete the SMS from the inbox for security manners (human rights, free to choose the candidate). This process was for one SMS, so the system will go back to inbox to handle another SMS in the same way than the first SMS did.



B. ***Internet Voting:*** The second method is internet based voting system through the website.The website consists of a number of pages, each page has its own features and implemented in (Kurdish and English) languages.

The two implemented voting system (SMS and Internet) are both connected to the same MySQL database. One conclude that the voter can vote through one of the two methods only one time and if he tries to vote again, the system will deny him. It also contains a special part for the admin which allows him to login into the dashboard of the website. Through this dashboard the Admin can change or add information on the website.



IV. ONLINE VOTING SYSTEM SECURITY LEVELS

For the security, a voice recognition technique is used because only the admin knows the correct word to choose and the admin can talk either in English or Arabic. (Google) machine translate is used as a tool for voice recognition. The recorded voice is sent to this machine through the internet, and the machine sends us back a listed text of the right words and the word that have similar syntax of the actual word. After that, the admin must choose the right word only he knows, and then the system connects to the server and get the information from the database in order to know how many votes each candidate has collected.

Other level of security that is used in this research is specified for the (database). One of the newest techniques that used is a Barcode Scanner. This technique is a specific type of (QR Code). In order to allow only specific people and authorized people to access, this part holds a specific (QR code).

V. CONCLUSION

This research paper proposed a real time online voting system based on android phones. The system is first analysed for both SMS and Internet based voting. It then developed by implementing both techniques using android platform. The usability of this system is very high if it will be used in real life election process. It will definitely helpful for the users who wish to vote and the voting process will be made very easy by using this application.

Advantages of the proposed online voting system: online voting minimizes the risk of ambiguities as the voter makes his choice by touching the screen. Online voting could also minimize the need for recounts as everything is tabulated by the computer.

Disadvantage of the proposed online voting system: online voting is not more secure as possible than the paper-ballot system. Electronic failures might occur with such a system. The online voting system that we developed is tested with 100 peoples holding Asia cell sim card. The results show that our system is very efficient and easy to use.

INDOOR NAVIGATION SYSTEM USING BLUETOOTH TECHNOLOGY

M.B.Prasanth Yokesh[#1], G.Anjana[*2], A.R.Dhivya[*3], B.Narmadha[*4]

[#1]*Assistant Professor , Anand Institute of Higher Technology, Chennai*
[*2] *Anand Institute of Higher Technology, Chennai*
[*3] *Anand Institute of Higher Technology, Chennai*
[*4] *Anand Institute of Higher Technology, Chennai*

Abstract—**In the past few years, a number of ideas have been proposed for indoor navigation systems. These ideas were not as widely implemented as outdoor positioning systems like GPS (Global Positioning Systems). We propose an indoor navigation assistance system using Bluetooth which is low cost and feasible to use in daily life. Our system enables users with handheld mobile devices to steer with ease through the indoor premises using the short range radio frequencies of Bluetooth. Dijkstra's algorithm is used to determine the shortest path from the source to the required destination.**

1. INTRODUCTION

The expedience and comfort provided by the existing outdoor navigation systems has facilitated the development of indoor navigation and location tracking.GPS positioning provided by mobile telephone operators are suitable for *outside* environments where clear line-of-sight with respect to the satellites or base stations is available. However, they suffer from multi-path effects within buildings, and therefore, in indoor they show poor performances [1].In recent times there has been a growth in huge infrastructures like shopping malls, industrial complexes along with existing structureslike hospitals and college campuses. Moving round in such premises can be difficult and finding the path to the desired location can be time consuming and tiresome.

The ideal indoor navigation system should provide easy guidance to navigate through such areas The signals used by outdoor locating technologies are often inadequate in this setting. Systems that rely on the use of cellular communication signals or identification of nearby Wi-Fi access points do not provide sufficient accuracy to differentiate between the individual rooms of a building. GPS is also used for the navigation purpose. Indoor tracking can also be done with the help of the wireless communication Wi-Fi.We decided to use Bluetooth technology to estimate the location because of its main hardware features: low power consumption, low cost and low interference with devices that work on the same frequency range and its widespread use in typical mobile devices [2].Desktop software built on Java platform would use Dijkstra's algorithm to determine the shortest path to the desired destination.

II .RELATED WORK

3D indoor location and navigation system based on Bluetooth: This paper presents the design and implementation on mobile device, of a 3D positioning and navigation system for indoor, based on the use of Bluetooth (BT) radio technology and implemented using Java and J2ME. This implementation is adaptable to many indoor environment (commercial centers, offices, museums, etc.) previously modeled and loaded. J2ME and Bluetooth Technology is the main features used. [2]

Low cost Bluetooth mobile positioning for location based application: This system has 2 main components namely the Bluetooth sensor system and Central Navigation System. The Bluetooth Sensor System allows mobile devices whose bluetooth mode is set to discoverable, to be scanned and detected, and they receive customizable text message and other relevant files (maps, sound files, video clips) of their positioning information, e.g. room identity. The positioning information is also sent to the Central Navigation System which in turn displays and updates the navigation map. The system is also used to track the movement of different BT mobile devices within the implemented environment. [3]

***Research of Indoor Local Positioning Based on Bluetooth Technology**:* Bluetooth is a technology with low-power, short-distance, wireless systems, can be used to construction awireless services of indoor. The development of local positioning services based on the Bluetooth technology is discussed in this paper. An approach based on the positioning information exchanged between the master and slave devices within the Bluetooth network.[4]

***Indoor Navigation Performance Analysis EPFL*:** The computation of the best route is based on a Dijkstra's algorithm which is specifically designed for a continuous and Oriented graph. The algorithm has to estimate the shortest path between a start node and an end node given by a user who has a specific profile. The best route computed by the system is used as input for the navigation process and for providing guidance information to the user [5].

Navizon I.T.S: This system locates Wi-Fi enabled devices. No application is required on the tracking device but the Wi-Fi radios should be on and within the coverage area of the network of nodes. The I.T.S(Indoor Triangulation system) site periodically reports the details about the Wi-Fi enabled devices. This system basically uses Wi-Fi to track devices using Navizon's proprietary algorithm with the help information collected by the nodes [6].

NFC (Near Field Communication)

At its core, all NFC is doing is identifying us. The technology is simple, but it's a short-range, low power wireless link that can transfer small amounts of data between two devices held a few centimeters from each other. This distance could be within a range of 10cm which is very less comparatively. Every time the user needs to find his location inside the campus, he/she will have to manually place their phones near the NFC tags. Also, there needs to be NFC chip inbuilt in the users Smartphone.

BLUETOOTH

An alternative for all above technologies is the use of Bluetooth. In this we develop an indoor navigation system on a Bluetooth-enabled smart phone. We propose the development of a new approach that uses data from the devices Bluetooth module to determine user position. A routing algorithm (DIJKSTRA, etc.) calculates the optimal path from user position to destination. Sufficient accuracy for navigation can be achieved at low costs. This technique shows promise for future handheld indoor navigation systems that can be used in malls, museums, hospitals, and college campuses.

II. SYSTEM ARCHITECTURE

OUR PROPOSED SYSTEM WORKS IN 2 MAIN MODULES:

1. Desktop Module
2. Mobile Module

Desktop Module: The desktop module that will be used by administrator ideally be doing the following:

- Set map information.
- Save/Load map information to/from files.
- Set Bluetooth device information.
- Set paths.
- Find optimum paths.
- Auto compiles mobile application.
- Upload mobile application to dedicated website for public download access.

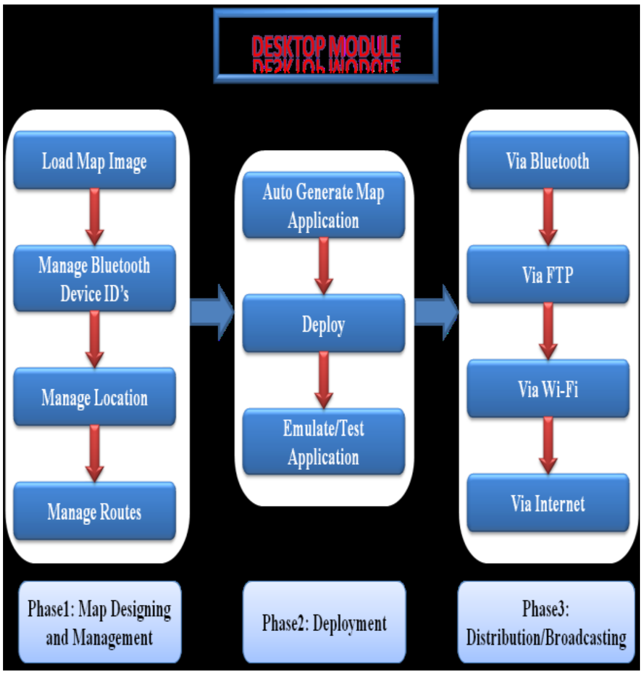


Fig-1: Desktop Module

Dijkstra's Algorithm

"S is a set of Bluetooth Devices, discovered Bluetooth devices, locations, routes, Dijkstras shortest Path.
S={B,B,L,R,Dsp}
Where, B= {b1, b2 ,…..bn} Set of Bluetooth devices.
B={b1,b2….bn} Set of discovered devices.
B B
L= {l1,l2,…..ln}Set of locations (set of vertices)
Lsp=Location start point
Lep=Location end point
Lsp, Lep L R= {r1, r2,….rn}Set of routes (set of edges)
Dsp= SP {L, R}
Where $Lsp=lsp1', lsp2',\ldots.lspn'$
Lsp L

Example:
The person has to go from the location L1 to L4.

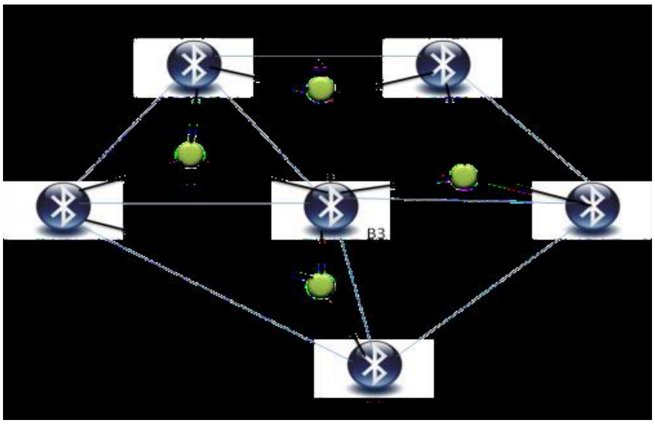


Fig-2: Dijkstra's implementation

Then the shortest path to reach L4 from L1 by using Dijkstra's algorithm is:

1. User selects his source as L1.
2. Also select destination as L4.
3. All distances from L1 to L4 are calculated.
4. The shortest possible distance from all the calculated ones is selected
5. All the paths from L1 to L4 are shown along with the shortest path as shown in figure (shortest path is shown with red line).

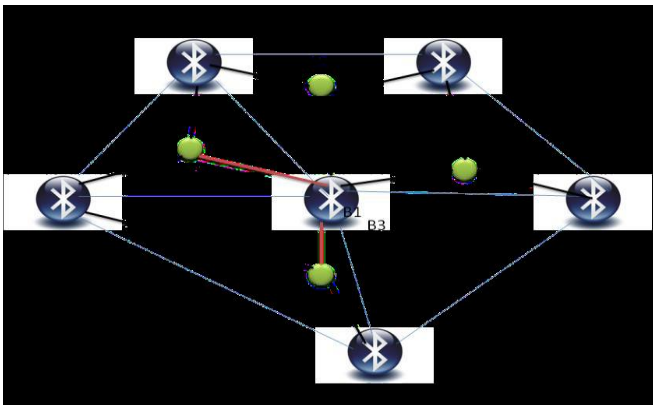


Fig-3: Dijkstra's implementation

The shortest path is L1-B3-L4

Mobile module: The mobile application that can be downloaded from internet by any user on his phone will show the user overall map of the premise. Apart from the application will allow the user to

- See his current location.
- Select source point.
- Select destination point.
- Show all paths from source to destination.
- Show shortest path from source to destination.
- Update current location at regular intervals.
- Graphically show the path overlay on premise map.
- Navigate through premise map for additional information.
- A set of Bluetooth devices placed at the various locations in the premises assist in determining the current location of the user.

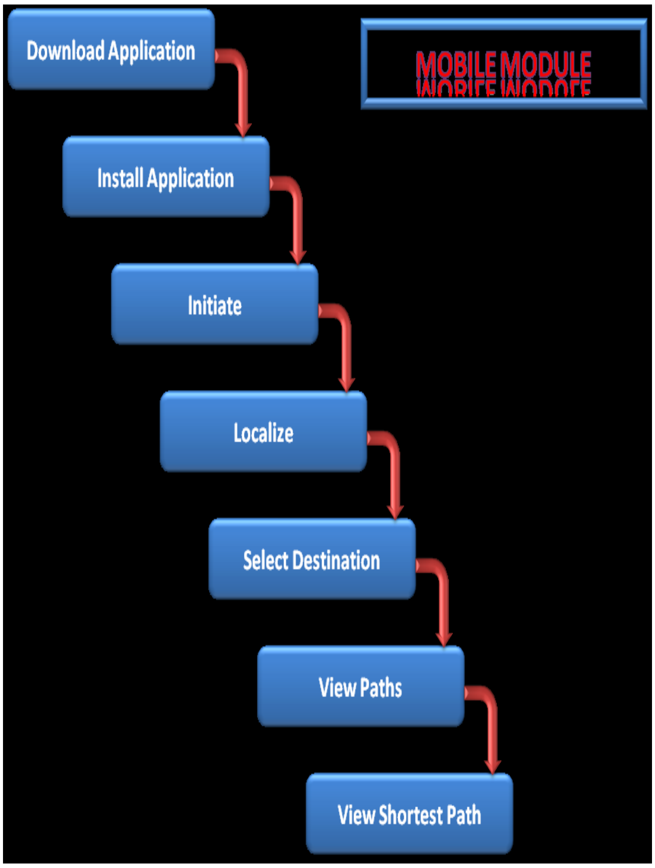


Fig-4: Mobile Module.

III. WORKING

1) Firstly all the application work i.e. the creation of the maps, managing all the paths, scaling of the maps, adding the Bluetooth devices, and managing the database is done by the Administrator on the desktop module.

2) This whole J2ME application is compiled and a jar file is created and ready to transfer to the user.

3) Whenever a user enters a premise with this system it is necessary that his mobile's Bluetooth is enabled. The server i.e. the desktop module will prompt the user a message through Bluetooth whether the latter wants the application or not, if yes the compiled J2ME application is sent to the user through Bluetooth.

4) Now the user has the jar file of the application. He has to run this application. The application helps the user to easily navigate through the premises. It shows the user his current position. The user can also find all possible paths from any sources place to destination and out of all this he can also find the shortest path to the destination.

5) The Bluetooth devices help the application to find the users current position and also the position is continuously updated as the user moves.

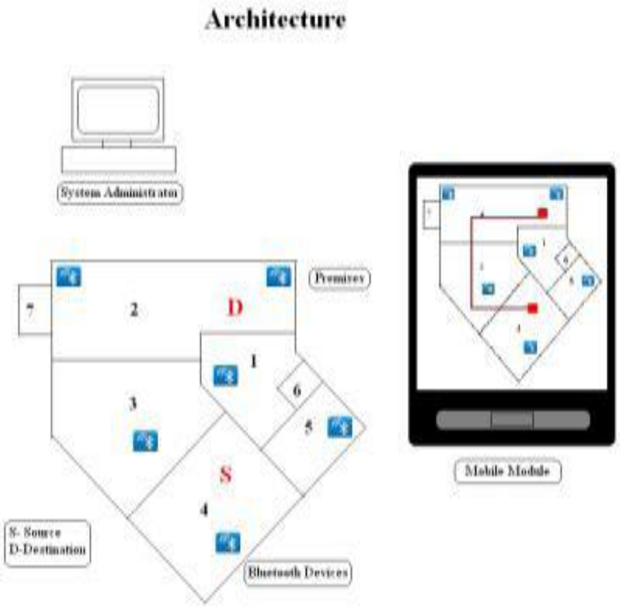


Fig-5: Architecture

WHY BLUETOOTH?

These are ultra-low cost Bluetooth devices that will be setup in premises at regular intervals. These devices will transmit their Device-ID to all Bluetooth devices in range. This is the only purpose these devices shall serve. These devices can also simultaneously be used for other purposes without affecting the navigation system at all.

The major advantages of using Bluetooth for indoor tracking are:

- Low power consumption.
- Low cost and low interference with devices that work on the same frequency range .
- widespread use in mobile devices

IV. CONCLUSION

This project has detailed the designing of an Indoor Map Guidance system via the use of portable mobile devices, with its application set on a smart indoor campus environment. It is a mobile application for Android platform with Bluetooth that allows the user to readily localize and view the map of the building on their Smart phones. The proposed system is also able to assist and guide visitors within any public buildings such as shopping malls, airports, hospital, museums, exhibition centers, schools and colleges. It utilizes modern technology such as Bluetooth. Bluetooth is platform independent and has high degree of standardization. It is widespread supported, has low cost and low power consumption. Also, the Bluetooth devices that we use have low interference with devices that work on same frequency range.

REFERENCES

[1]. Omran Al Hammadi, Ahmed Al Hebsi, M. Jamal Zemerly , "Indoor Localization and Guidance using Portable Smartphones"

[2]. Jing Hang Choo, Soon Nyean Cheong, Yee Lien Lee, and Sze Hou The," I2Navi: An Indoor Interactive NFC Navigation System for Android Smartphones"

[3]. G. M. Miraz, I. L. Ruiz, and M. A. Gomez Nieto,"How NFC Can Be Used for the Compliance of European Higher Education Area Guidelines in European Universities," in 2009 First International Workshop on Near Field Communication, 2009, pp. 3–8. World Academy of Science, Engineering and Technology 72 201273

[4]. Nagesh Potdar, Dipak Pawar, Sachin Jain, Bhumil Haria, Seema Shrawne," Indoor Navigation Using Smartphones"

[5]. Omar Cruz *, Erik Ramos †, and Moisés Ramírez," 3D Indoor Location and Navigation System Based on Bluetooth"

[6]. http://www.micello.com/products/maps on 15 April 2012.

[7]. http://www.fastmall.com/ on 15 April 2012.

[8]. https://www.google.co.in/#q=indoor+navigation+android

[9]. https://www.google.co.in/#q=how+bluetooth+works

[10].https://www.google.co.in/#q=indoor%20 navigation%20using%20 bluetooth

[11]. https://www.google.co.in/#q=dijkstra%27s+algorithm

[12]. https://www.google.co.in /#q=how+ wifi+works+f or+ indoor +navigation

[13]. E. W. Dijkstra, "A Note on Two Problems in Connexion with Graphs.,"Numerische Mathematlk 1, pp. 269-271, 1959.

AUTOMATED AGRICULTURE MONITORING AND CONTROL USING WIRELESS SENSORS

Mr. .M. Rajkannan[*1], Mrs. K. Rejini[*2], Mrs.Amsavalli[*3], Mr.AS.Balaji[*4]

[#1]*PG Student, Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai.*
[*2,*3,*4]*Assistant Professor, Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai.*

***Abstract* - An automated agriculture system was developed to optimize water use for agricultural crops. The system has a distributed wireless network of soil-moisture and temperature sensors placed in the root zone of the plants. In adding, a gateway unit handles sensor information, triggers actuators, and transmits data to a web application. An algorithm was developed with threshold values of temperature and soil moisture that was programmed into a microcontroller-based gateway to control water quantity. The system was powered by photovoltaic panels and had a duplex communication link based on a Cellular-Internet interface that allowed for data inspection and agriculture scheduling to be programmed through a web page. If its energy autonomy and low cost, the system has the potential to be useful in water limited geographically isolated areas.**

Index Terms-**Automation, cellular networks, Internet, agriculture, measurement, water resources, wireless sensor networks (WSNs).**

I. INTRODUCTION

AGRICULTURE uses 85% of available freshwater resources worldwide, and this percentage will continue to be dominant in water consumption because of population growth and increased food demand. There is an urgent need to create strategies based on science and technology for sustainable use of water, including technical, agronomic, managerial, and institutional improvements. An agriculture monitoring and control system was developed to optimize water use for agricultural crops. The system has a distributed wireless network of soil-moisture, temperature sensors and Humidity sensor placed in the e plants. In addition, a gateway unit handles sensor information, triggers actuators, and transmits data to a web application. An algorithm was developed with threshold values of temperature and soil moisture that was programmed into a microcontroller-based gateway to control water quantity. The system was powered by photovoltaic panels and had a duplex communication link based on a cellular Internet interface that allowed for data inspection and agriculture development to be Because of its energy autonomy and low cost, the system has the potential to be useful in water limited in nature isolated areas

This paper, the development of the deployment of an automated agriculture system based on microcontrollers and wireless communication at experimental scale within rural areas is presented. The aim of the implementation was to demonstrate that the automatic agriculture can be used to reduce water use. The implementation is a photovoltaic powered automated agriculture system that consists of a distributed wireless network of soil moisture and temperature sensors deployed in plant root zones. Each sensor node involved a soil-moisture probe, a temperature probe, a microcontroller for data acquisition, and a radio transceiver; the sensor measurements are transmitted to a microcontroller-based receiver. This gateway permits the automated activation of agriculture when the threshold values of soil moisture and temperature are reached. Communication between the sensor nodes and the data receiver is via the Zigbee protocol under the IEEE 802.15.4WPAN. This receiver unit also has a duplex communication link based on a cellular-Internet interface, using general packet radio service (GPRS) protocol, which is a packet-oriented mobile data service used in 2G and 3G cellular global system for mobile communications (GSM). The Internet connection allows the data inspection in real time on a website, where the soil-moisture and temperature levels are graphically displayed through an application interface and stored in a database server. This access also enables direct programming of scheduled agriculture schemes and trigger values in the receiver according the crop growth and season management. Because of its energy autonomy and low cost, the system has potential use for organic crops, which are mainly located in geographically isolated areas where the energy grid is far away.

In a wireless node, the radio modem is the major power consuming component; recently, wireless standards have been established with medium access control protocols to provide multitask support, data delivery, and energy efficiency performance such as the standards for wireless local area network, IEEE 802.11b (WiFi) and wireless personal area network (WPAN), IEEE 802.15.1 (Bluetooth) IEEE802.15.3, and IEEE 802.15.4 (ZigBee) and those open wireless communication standards for Internet protocol version 6 (IPv6) over low-power wireless personal area networks WPAN wireless highway addressable remote transducer Wireless HART developed

In this paper, the development of the deployment of an automated agriculture system based on microcontrollers and wireless communication at experimental scale within rural areas is presented. The aim of the implementation was to demonstrate that the automatic agriculture can be used to reduce water use. The implementation is a photovoltaic powered automated agriculture system that consists of a distributed wireless network of soil moisture and temperature sensors deployed in plant root zones. Each sensor node involved a soil moisture probe, a temperature probe, a microcontroller for data acquisition, and a radio transceiver; the sensor measurements are transmitted to a microcontroller-based receiver.

This gateway permits the automated activation of agriculture when the threshold values of soil moisture and temperature are reached. Communication between the sensor nodes and the data receiver is via the Zigbee protocol under the IEEE 802.15.4WPAN. This receiver unit also has a duplex communication link based on a cellular-Internet interface, using general packet radio service (GPRS) protocol, which is a packet-oriented mobile data service used in 2G and 3G cellular global system for mobile communications (GSM). The Internet connection allows the data inspection in real time on a website, where the soil-moisture and temperature levels are graphically displayed through an application interface and stored in a database server. This access also enables direct programming of scheduled agriculture schemes and trigger values in the receiver according the crop growth and season management. Because of its energy autonomy and low cost, the system has potential use for organic crops, which are mainly located in geographically isolated areas where the energy grid is far away.

II. MOTIVATION OF RESEARCH

In environmental applications, sensor networks have been used to monitor a variety of environmental parameters.

- ❖ Humidity, temperature level and water flow.
- ❖ Power management has been addressed in both hardware and software.
- ❖ Data inspection in real time on a website.

III. LITERATURE SURVEY

[1] Yuan, Y. Luo, X. Sun, and D. Tang, proposed the system of soil surface can have on CWSI calculated by the Jackson energy balance method. CWSI calculated under condition in which the ware soil surface is viewed by IRT method.

[2] L. M. Oliveira and J. J. Rodrigues proposed the environmental monitoring is achieved by a small number of expensive and high precision sensing unities. Collected data are retrieved directly from the equipment at the end of the experiment and after the unit is recovered. The implementation of a wireless sensor network provides an alternative solution by deploying a larger number of disposable sensor nodes.

[3] D.-M. Han and J.-H. Lim, designs smart home device descriptions and standard practices for demand response and load management “Smart Energy” applications needed in a smart energy based residential or light commercial environment. The control application domains included in this initial version are sensing device control, pricing and demand response and load control applications. This paper introduces smart home interfaces and device definitions to allow interoperability among ZigBee devices produced by various manufacturers of electrical equipment, meters, and smart energy enabling products.

[4] D. D. Chaudhary, S. P. Nayse, and L. M. Waghmare proposed MEMS technology for hardware, some other technologies like, satellite sensing, Remote Sensing, Global Positioning System and Geographical Information System are also contributing in overall progress. Beckwith et al. had worked on WSN in large scale vineyard on very large scale design and deployment.

[5]. J. Lin, W. Xiao, F. L. Lewis, and L. Xie, proposed the has many advantages, including the miniaturization of sensor nodes, easy deployment, low cost, and tolerance to fault conditions. Target tracking is one of the most important applications of WSNs, in which, due to the limited resources for sensing, communication, and computation, the network must rely on sensor management to balance the tracking accuracy and energy consumption.

IV. CONCLUSION OF LITERATURE SURVEY

The automated irrigation system implemented is a cost effective alternative for agriculture. The WIU average current consumption because of the electronic components was of low in operational mode. Several automated irrigation periods were carried out by the system because of the soil-moisture or temperature levels, regardless of the scheduled irrigation. All data were uploaded each hour to the web server for remote supervision.

V. MODEL CONSTRUCTION

The automated agriculture system hereby reported, consisted of two components (Fig. 1), wireless sensor units (WSUs) and a wireless information unit (WIU), linked by radio transceivers that allowed the transfer of soil moisture and temperature data, implementing a WSN that uses ZigBee technology. The WIU has also a GPRS module to transmit the data to a web server via the public mobile network. The information can be remotely monitored online through a graphical application through Internet access devices.

A. Wireless Sensor Unit

A WSU is comprised of a RF transceiver, sensors, a microcontroller, and power sources. Several WSUs can be deployed in-field to configure a distributed sensor network for the automated agriculture system. Each unit is based on the microcontroller. The microcontroller was programmed in C compiler.

The data are packed with the corresponding identifier, date, and time to be transmitted via XBee radio modem using a RS-232 protocol through two digital ports configured as transmitter and receiver respectively.

B. **Wireless Information Unit**

The soil moisture and temperature data from each WSU are received, identified, recorded, and analyzed in the WIU. The WIU consists of a master microcontroller a GPRS module an RS-232 interface two electronic relays, two 12 V dc Live well pumps for driving the water of the tanks. The functionality of the WIU is based on the microcontroller, which is programmed to perform diverse tasks.

The WIU is ready to transmit via XBee the date and time for each WSU once powered.Then, the microcontroller receives the information package transmitted by each WSU that conform the WSN. GPRS modem includes an embedded transmission control protocol/Internet protocol stack to bring

Internet connectivity, a UFL antenna connector and subscriber identity module (SIM) socket.

The module is capable of transfer speeds. Graphical user interface software was developed for real time monitoring and programming of agriculture based on soil moisture and temperature data. The software application permits the user to visualize graphically the data from each WSU.

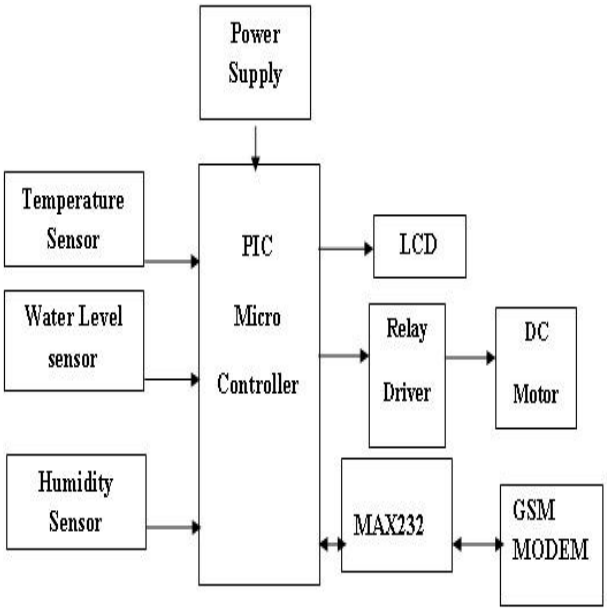


Figure 1 Architecture for Automated Agriculture Monitoring System

VI. CONCLUSION

The automated agriculture system implemented was found to be feasible and cost effective for optimizing water resources for agricultural production. This agriculture system allows cultivation in places with water scarcity thereby improving sustainability. The automated agriculture system developed proves that the use of water can be diminished for a given amount of fresh biomass production. The use of solar power in this agriculture system is pertinent and significantly important for organic crops and other agricultural products that are geographically isolated, where the investment in electric power supply would be expensive.

The agriculture system can be adjusted to a variety of specific crop needs and requires minimum maintenance. The modular configuration of the automated agriculture system allows it to be scaled up for larger greenhouses or open fields. In addition, other applications such as temperature monitoring in compost production can be easily implemented. The Internet controlled duplex communication system provides a powerful decision making device concept for adaptation to several cultivation scenarios. Furthermore, the Internet link allows the supervision through mobile telecommunication devices, such as a Smartphone.

REFERENCES

[1] G. Yuan, Y. Luo, X. Sun, and D. Tang, “Evaluation of a crop water stress index for detecting water stress in winter wheat in the North China Plain,” *Agricult. Water Manag.*, vol. 64, no. 1, pp. 29–40, Jan. 2004.

[2] L. M. Oliveira and J. J. Rodrigues, “Wireless sensor networks: A survey on environmental monitoring,” *J. Commun.*, vol. 6, no. 2, pp. 143–151, Apr. 2011.

[3] D.-M. Han and J.-H. Lim, “Smart home energy management system using IEEE 802.15.4 and ZigBee,” *IEEE Trans. Consum. Electron.*, vol. 56, no. 3, pp. 1403–1410, Aug. 2010.

[4] D. D. Chaudhary, S. P. Nayse, and L. M. Waghmare, “Application of wireless sensor networks for green house parameters control in precision agriculture,” *Int. J. Wireless Mobile Netw.*, vol. 3, no. 1, pp. 140–149, Feb. 2011.

[5] J. Lin, W. Xiao, F. L. Lewis, and L. Xie, “Energy-efficient distributed adaptive multisensor scheduling for target tracking in wireless sensor networks,” *IEEE Trans. Instrum. Meas.*, vol. 58, no. 6, pp. 1886–1896.

AVOID RAILWAY ACCIDENTS USING WIRELESS SENSOR NETWORKS

M. Mercy[#1], Mr. A.S Balaji[*2], Mr. D. Rajini girinath[*3], Mrs. P. Suthanthira Devi[*4]

[#1* 3]*PG Student, Dept. of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai.*
[*2,* 4] *Assistant Professor, Dept. of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai.*

***Abstract*- In recent years, the range of sensing technologies has expanded rapidly, whereas sensor devices have become cheaper. This has led to a rapid expansion in condition monitoring of systems, structures, vehicles and machinery using sensors. Key factors are the recent advances in networking technologies such as wireless communication and mobile ad hoc networking coupled with the technology to integrate devices. Wireless sensor networks(WSN) can be used for monitoring the railway infrastructure such as bridges, rail tracks, track beds, and track equipment along with vehicle health monitoring such as chassis,bogies,wheels and wagons. Condition monitoring reduces human inspection and reduces maintenance through detecting faults before they escalate, and improves safety and reliability. This is vital for the development, upgrading, and expansion of railway networks. These wireless sensors network technology for monitoring in the railway industry for analyzing system, structures, vehicles and machinery. Condition monitoring detects and identifies deterioration in structures and infrastructure before the deterioration causes a failure or prevents rail operations. In simple condition monitoring, sensors monitor the condition of a structure or machinery. If the sensor readings reach a predetermined limit or fault condition, then an alarm is activated. However, this simplistic approach may lead to a large number of false alarms and missed failures. In now a days the track information send to the base station. Base station information send to the train using LCD,APR If any railway accidents send to the ambulance.**

***Index Terms*-Condition monitoring, wireless sensor network (WSN), maintenance engineering, railway engineering, event detection, Base station.**

I. INTRODUCTION

In recent years, the range of sensing technologies has expanded rapidly, whereas sensor devices have become cheaper. This has led to a rapid expansion in condition monitoring of systems, structures, vehicles, and machinery using sensors. Key factors are the recent advances in networking technologies such as wireless communication and mobile ad hoc networking coupled with the technology to integrate devices. Wireless sensor networks (WSNs) can be used for monitoring the railway infrastructure such as bridges, rail tracks, track beds, and track equipment along with vehicle health monitoring such as chassis, bogies, wheels, and wagons. Condition monitoring reduces human inspection requirements through automated monitoring, reduces maintenance through detecting faults before they escalate, and improves safety and reliability. It reduces the human inspection compared with manual inspection.

A key part of the management will be condition monitoring. Condition monitoring detects and identifies deterioration in structures and infrastructure before the deterioration causes a failure or prevents rail operations. In simple condition monitoring, sensors monitor the condition of a structure or machinery. If the sensor readings reach a predetermined limit or fault condition, then an alarm is activated. This approach may lead to a large number of false alarms and missed failures. It only provides local analysis but does not take advantage of the superior capabilities when the sensors are networked and their data processed collectively.

WSN monitoring provides continuous and near real-time data acquisition and autonomous data acquisition (no supervision is required); increased frequency of monitoring compared with manual inspection; improved data accessibility, data management, and data use compared with non-networked systems as all data can be collected and processed centrally; the ability to combine data from a wide variety of sensors; intelligent analysis of data to “predict and prevent” events using intelligent algorithms; the ability to turn data into information about the status of important structures, infrastructure and machinery; and, a global data view that allows trending information to be determined where degradation is happening slowly over a relatively long period of time.

WSN monitoring can be used to:

1. Maintain process tolerance;
2. Verify and protect machine, system and process stability;
3. Detect maintenance requirements;
4. Minimize downtime;

There are number of challenges with WSN. They generate large amounts of data at rapid rates and often on an ad hoc basis. Data may be produced from multisource that has to be fused. The system and structures monitored using sensors often exhibit complex behavior, which is difficult to understand and interpret. Hence the data must be carefully managed to provide a view of the system status. Sensor data are very noisy and sensors themselves can become defective wherever they are installed. Sensor data may contain errors, particularly where the sensors are subject to harsh conditions as this exacerbates sensor and communication failures. Sensor networks often have to be installed in challenging environments to be able to monitor structures and infrastructure. Wireless sensor used condition monitoring. WSNs need to minimize energy usage yet communication needs to be maximally efficient and communication requires energy. If there are errors in transmission across the WSN, then data may be missing.

II. MOTIVATION OF RESEARCH

The motivation on my research is to increase the safety and reliability with low cost using wireless sensor networks.

1.How to provide safety and reliability?
2.How to reduce human inspection?
3.How to avoid the accidents?

III. LITERATURE SURVEY

1. Y. Sankarasubramaniam, and E. Cayirci (2002) Says that sensor networks which has been made viable by the convergence of micro electro-mechanical systems technology, wireless communications and digital electronics. First, the sensing tasks and the potential sensor networks applications are explored, and a review of factors influencing the design of sensor networks is provided. It has low power and low memory.

2. Kemal Akkaya and Mohamed Yuns(2005) Says that recent routing protocols for sensor networks and presents a classification for the various approaches pursued. The three main categories explored that are data-centric, hierarchical and location-based. It based Qos methodology is followed. Data centric method followed many of researches.

3. D. Brake and W. Chiu (2005) Says that a benefit of wireless structural monitoring systems is that they are inexpensive to install because extensive wiring is no longer required between sensors and the data acquisition system. It has low power consumption.

4. E. Aboelela, and W. Edberg (2006) Says that the current state of the art in detecting immediate and long-term railway track problems involves both inspectors walking the track lines and train cars instrumented with accelerometers and ultrasonic sensors that are capable of detecting wear of the rail and breakages , it propose a fundamentally different approach to improve the current practices in railway operations using wireless sensor network.

5. M. Aguado (2008) Says that Routing protocols are in charge of discovering and maintaining the routes in the network. Protocol mainly depends on the capabilities of the nodes and on the application requirements. wi-max presents a review of the main routing protocols proposed for wireless sensor networks. Additionally, it includes the efforts carried out by Spanish universities on developing optimization techniques in the area of routing protocols for wireless sensor networks.

6. V.E. Balsa, *and* L.C. Jain(2010) Says that a necessary strategy to improve our technologies is to provide them with useful pieces of deterministic previous knowledge about the processes and the equipment. Our attention was previously focused on the industrial control systems, implemented with low level devices (controllers, sensors, actuators), that need knowledge on the specific controlled plants as well as on the general theoretical foundations. The advantages are high reliability, good precision.

7.A. Anastasopoulos, and K. Bollas (2010) Says that the ever-increasing demand for safer, faster and cleaner surface transportation such as railway, imposes heavy usage and loads on train axes and wheels. Such components, during usage, are subjected to complex, fatigue loading, shock loads, impacts, bending, etc. and/or combinations of the above. Train wheel and axle failures while train is in operation occasionally lead to catastrophic failures, possibly with human victims. It presents the raw data and evaluation results from AE experiments on train and tram wheels, (both healthy ones and wheels containing known defects). During measurements different AE sensors were placed on the side of the rails while the ail cars or trams were passing at different speeds.

8. Kalpana Sharma, and Jagdish Kumawat (2014) says that railways are large infrastructures and are the prime mode of transportation in many countries. Even a small improvement in performance of railways has significant economic benefits to rail industry. Thus, a proper maintenance strategy is required to govern optimization of inspection frequency and/or improvement in skill and efficiency. It is different kinds of rail defects inspection and maintenance methods are described and a basic algorithm is readdressed that makes use of wireless acoustic sensors for detecting cracks and breakages in the railway tracks.

9. Eduardo Cañete , and Jaime Chen(2015) says that Recently, slab track systems have arisen as a safer and more sustainable option for high speed railway infrastructures, compared to traditional ballasted tracks. Integrating wireless Sensor Networks within these infrastructures can provide structural health related data that can be used to evaluate their degradation and to not only detect failures but also to Predict. It is different communication architectures are designed and tested to select the most suitable system meeting such requirements as efficiency, low cost and data accuracy.

10.Michael Weeks, and Anthony Moulds (2015) says that In recent years, the range of sensing technologies has expanded rapidly, whereas sensor devices have become cheaper. This has led to a rapid expansion in condition monitoring of systems, structures, vehicles, and machinery using sensors. Condition monitoring reduces human inspection requirements through automated monitoring, reduces maintenance through detecting faults before they escalate, and improves safety and reliability. In simple condition monitoring, sensors monitor the condition of structure or machinery. If the sensor readings reach a predetermined limit or fault condition, then an alarm is activated. However, this simplistic approach may lead to a large number of false alarms and missed failures.

IV. CONCLUSION OF LITERATURE SURVEY

WSNs used for condition monitoring in the railway industry sensors are objective and can provide data from the entire object to allow the whole object's health to be fully assessed and to analyze its durability and remaining life time. The main challenge for WSNs in railway applications is determining the best measurement technologies to use. The WSN must be reliable and accurate to enable effective condition monitoring in harsh and inaccessible environments but must also be cost effective.

V. WIRELESS SENSOR NETWORK SETUP

WSN setup for railway condition monitoring. Sensor devices are mounted on boards attached to the object being monitored; examples include track, bridges, or train mechanics. One or more sensors are mounted on a sensor board (node). The sensor nodes communicate with the base station using a wireless transmission protocol; examples include Bluetooth and Wi-Fi. The base station collates data and transmits it to the control center server possibly through satellite or GPRS. There are variations on this setup. In some systems, the sensor nodes may communicate directly with the server rather than via the base station. In other systems, the user accesses the data directly via the base station. The base station information access only the administrator. The admin only announced track information to each railway stations .

VI. BLOCK DIAGRAM

Weather sensors are attached in the railway track. Weather sensor examples temperature, rain, and flex sensors. The sensors sense if any faults, cracks, obstacles of the information send to the base station using wireless communication. Wireless examples ,Bluetooth and Wi-Fi. The base station information send to the server and also database. The administrator access the server and information send to all railway station. And base station information send train. Inside the train GSM mode is fixed.

If any fault information send to the of LCD display and voice message of APR. GSM is used message passing. GPS used find the fault location. If any accidents occur the information send to the ambulance. The scope of this work is to achieve avoid the railway accidents and improve safety reliability. Reduce human inspection and save cost reliability. Reduce cost and time. . The base station collates data and transmits it to the control center server possibly through satellite or GPRS. There are variations on this setup. In some systems, the sensor nodes may communicate directly with the server rather than via the base station. In other systems, the user accesses the data directly via the base station. The base station information access only the administrator. The admin only announced track information to each railway stations

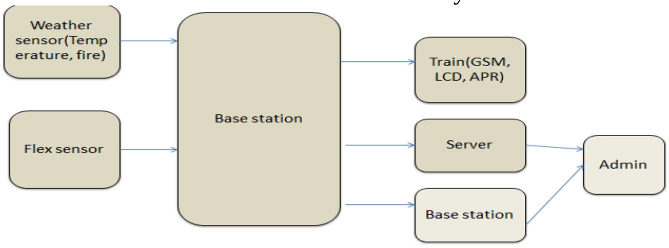


Fig 2:WSN using sensors

VII. SENSOR NODES

Multiple sensors may be mounted on the node. The microcontrollers used in sensors nodes are ultralow power microcontrollers to conserve energy. The boards generally comprise one or more wireless sensors. A microcontroller, transceiver, data storage and a power source.Memory , microcontroller, transceiver must be more powerful.

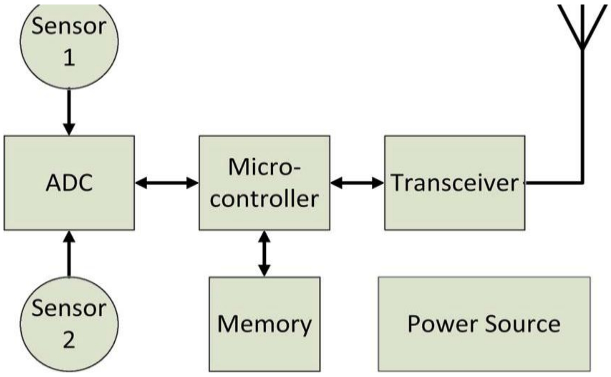


Fig 4:Composition of a typical sensor nodes

VIII. OBJECTIVE

Our paper surveys these wireless sensors network technology for monitoring in the railway industry for analyzing systems, structures, vehicles, and machinery. This paper focuses on practical engineering solutions, principally, which sensor devices are used and what they are used for; and the identification of sensor configurations and network topologies. To avoid the railway accidents. And also reduce human inspection. Improve safety.

The scope of this work is to achieve avoid the railway accidents and improve safety reliability. Reduce human inspection and save cost reliability. Reduce cost and time.

Potential applications of sensor networks include:

- Military Application
- Automated and smart homes
- Industrial automation
- Medical device monitoring
- Monitoring of weather conditions
- Robot control.
- Area monitoring
- Air quality monitoring
- Environmental magnitudes
- Industrial monitoring
- Machine health monitoring
- Industrial sense and control applications

There are a number of further research in condition monitoring in the railways. If the railway under sensors are attached and also the web camera and ip address based is fixed Then any faults occur in the information send to the train and base station using GSM and wireless for examples wireless Bluetooth and Wi-Fi. Web camera is used exactly known the picture for fault location .GPS used find the fault location . One or more times GPS find one location is fault location then information is passed to all trains go slow this accident zone.

IX.CONCLUSION

WSN used for condition monitoring in the railway industry. The emphasis is on practical engineering solutions. Sensor devices are used and what they are used for and identification of sensor nodes configuration and network topologies. Sensor devices have become cheaper. To avoid the railway accidents and improve safety and reliability. It reduce the human inspection .Reduce cost and time.

X. FUTURE RESEARCH

There are a number of further research in condition monitoring in the railways. If the railway under sensors are attached and also the web camera and ip address based is fixed. Then any faults occur in the information send to the train and base station using GSM and wireless for examples wireless Bluetooth and Wi-Fi. Web camera is used exactly known the picture for fault location .GPS used find the fault location . One or more times GPS find one location is fault location then information is passed to all trains go slow this is accident zone.

REFERENCE

[1] I.Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114,Aug. 2002.

[2] K. AK kaya and M.Younis, "A survey on routing protocols for wireless sensor networks," *Ad Hoc Netw.*, vol. 3, no. 3, pp. 325–349, Dec. 2005.

[3] D. Barke and W. Chiu, "Structural health monitoring in the railway industry: A review," *Struct. Health Monitoring*, vol. 4, no. 1, pp. 81–93, Mar. 2005

[4] E. Aboelela, C. Papakonstantinou, and V. Vokkarane, "Wireless sensor network based model for secure railway operations," in *Proc. 25th IEEE Int. Perform* 2006

[5] M. Aguado *et al.*, "WiMax on rails: A broadband communication architecture for CBTC systems," *IEEE Veh. Technol. Mag.*, vol. 3, no. 3, pp. 47–56, Sep. 2008.

[6] V. Balas and L. Jain, "World knowledge for sensors and estimators by models and internal models," *J. Intell. Fuzzy Syst.*, vol. 21, no. 1, pp. 79– 88, Apr. 2010.

[7] A. Anastasopoulos, K. Bollas, D. Papasalouros, and D. Kourousis, "Acoustic emission on-line inspection of rail wheels," in *Proc. 29th Eur. Conf. Acoust. Emission Testing*, Wien, Austria, 2010, pp. 1–8.

[8] Kalpana Sharma, Jagdish Kumawat "Railway Security System based on Wireless Sensor Networks: State of the Art" in*) Volume 96 No.25, June 2014.*

[9] Eduardo Cañete ,Jaime Chen"UsingWireless Sensor Networks and Trains as Data Mules to Monitor Slab Track Infrastructures" ISSN 1424-8220,in oct.2015.

[10] Michael Weeks, and Anthony Moulds "Wireless Sensor Networks for Condition Monitoring in the Railway Industry: A Survey" IEEE transactions on intelligent transportation systems, vol. 16, no. 3, june2015.

EFFICIENT METHOD TO RECORD THE AUDIO AND VIDEO OF CRASH SCENARIOS USING E-CRASHCODER

Nithiya[#1], A.Malathi[*2],A.Ruth Thabitha[*3],R.Femila Goldy[*4]

[#1]*PG Student, Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai.*
[*2,*3,*4]*Assistant Professor, Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai.*

***Abstract*- Intelligent Transportation System (ITS) is the utilization of information technology to enhance the transportation system. Elements within the transportation system such as vehicles, roads, traffic lights, and message signs, become smart devices.Traffic management on the road has become a severe problem of today's society because of growth of the urbanization, industrialization and population; there has been a tremendous growth in the traffic. With growth in traffic, there is occurrence of bundle of problems too; these problems include traffic jams, accidents and traffic rule violation at the heavy traffic signals. This in turn has an adverse effect on the economy of the country as well as the loss of lives. So problem given above will become worst in the future.Traffic lights play an important role in traffic management. Traffic lights are the signaling devices that are placed on the intersection points and used to control the flow of traffic on the road.The Intelligent Transportation system must offer efficient vehicular accident management distributedsystem. One of the most capabilities of this distributed system is efficient video recording of accident. Every year many accidents happen causing injuries and fatalities. For example, the road injury statistics in Yemen from 2001 to 2010 indicate that around 129,946 vehicles accident, 166,744 people incurred serious injuries, and 25,441 people die.Two design goals of accident management are: 1) Fast accident detection to decrease the delay associated with saving injuries and give them medical help. 2) Record the information associated with accident: The information recorded before and during the accident can be used by police investigator to understand the accident cause. It also can be used as evidence on law enforcement when a traffic accident occurred.**

***IndexTerms* - E-Crashcoder,Micro controller, GPS, GSM, Zigbee, DC motor, camera, vibration sensor.**

I. INTRODUCTION

The Crash Data Retrieval (CDR Tool) is a combination of hardware and software that reads the crash data found in a vehicles' Event Data Recorder (EDR).The EDR, a name coined by the National Highway Transportation Safety Administration (NHTSA),was developed to obtain the information needed to reduce deaths, injuries, and property damage due to vehicle crashes on the nation's highways. EDRs give goverment researchers and investigators information with which they can assess motor vehicles crashes in real world events with real So even though it was developed for one purpose, it's a valuable tool for another purpose.To design a next generation Vehicle Black Box (EDR), named as E-Crashcorder, (Enhanced Crash Data Recorder) that is the combination of all the advantages of previous Black Boxes, Event Data Recorders (EDRs) and standalone Digital Video/Audio recorders. The E-Crashcorder is integrated within the Electronic Control Unit (ECU) which is responsible for the airbag control and deployment and stores the status of vehicle gathered from different sensors. It is equipped with camera that records the video snapshots in front of the vehicle. It also records the audio inside the vehicle, using a microphone. The E-Crashcorder has Global Positioning System(GPS) receiver for reading the current latitude and longitude of the vehicle point. The 6 Degrees of Freedom (DOF) of inertial sensor, which is a Triple-axis accelerometer sensor and Triple-axis magnetometer sensor, is integrated with E- Crashcorder to read the velocity, acceleration and orientation of vehicle using which we analyze the stability of vehicle during the travel. After collecting and synchronizing all data, the E-Crashcorder saves them in Secure Digital (SD) Card. It has a USB port which is used to transfer the recorded data to a PC/Laptop the crash event. Immediately after a crash event, the recorder automatically stops after a few seconds. EDR data can be retrieved and analyzed to determine the driver's actions and how the vehicle performed at the time of a crash. A real time clock running in the microcontroller is used to timestamp every data that will be recorded. Here is the list of the crash data parameters that will be recorded. The system can be integrated with even bicycles/two wheelers with a few modifications.40 seconds of data recording that exceeds the traditional EDR limit of 10 seconds.A high performance 32-bit ARM cortex-M3 microcontroller consuming very low power. GPS & GSM works together in ensuring vehicle safety. It is programmed in such a way that whenever the collision occurs the location of vehicle is sent to registered telephone number through GSM & police to investigate. EDRs are a rapidly evolving and, in many ways, still immature technology. Both the Society of Automotive Engineers and the Institute of Electrical and Electronics Engineers have recently released standards or recommended practices for EDRs. EDR is to record speed, temperature, time and location of your car and second one will help to retrieve exactly what happened during the crash from the data stored in hard drive.

II. MOTIVATION OF RESEARCH

The motivation of my research is to reduce and prevent the roadway accident.

- How much data is collected?
- How to provide a safety?

III. LITERATURE SURVEY

1.Joe T.Correia,Ken A.Illiadis,Ed S.Mccarron (2001) explains that evolution of automatic recording devices in transportation using Event data recorders(EDR).It includes recording and retrieval of data in GM and vetronix systems are examined with particular attention on using the data for reconstruction purposes.

2.Anoop Mathew, Joseph Kuncheria, Yadukrishnan S, Gifty Raju, Haritha Chandrasekhar(2014) says that Car black box is an Event Data Recorder. When two cars collide, the sensor detects an accident and stores information regarding the car's speed, whether the seatbelts are fastened, the status of indicators and headlights and whether the driver hit the brakes before a collision. The number plate of the nearby vehicle is extracted from the captured images when accident was detected and the data is stored.

3.Mohamad Sigari,Muhammad-Reza Pourshahabi Mohsen Soryani and Mahmood Fathy(2014) says that review on driver face monitoring systems for fatigue and distraction detection is presented. It includes the position of eyelid distance, eye blink rate, blink speed, gaze direction, eye saccadic movement, yawning, head nodding and head orientation.

4.Mr.KishorRane,Mr. Rahul Tichkule, Mr.Mohit Shinde,Prof. S.I.Nipanikar(2014) explains that to develop the Embedded controller for Car Black Box using SoC (System on Chip) technique. System on Chip (SoC) is the effective method to implement embedded system like car black box, which consists of processor, various sensors like temp , eye blink , stearing position , over speed , alcohol sensors , SD card (to store the data) ,GPS and GSM.A car black box implemented on a single chip can reduce its size, power consumption and the cost.

5.Ramchandra Patil,Mr.Shivaraj(2014) says that to avoid the collision using UART and ARM. UART (Universal Asynchronous Receiver Transmitter) is the common peripheral found on microcontrollers widely used for communication with the external devices and systems. It includes Vehicle to Vehicle Collision Avoidance Unit (VVCAU) is used to avoid crashing between vehicles and Black Box (BB) records the relevant details about a vehicle such as Engine Temperature, Distance from obstacle, Speed of vehicle, Brake status, CO 2 Content, Alcohol content, Accident Direction, trip Time and Date.

6.Mr.Abhijeet M.Tote Dr. Khanapurkar (2014) explains that collection of the real time data after the detection of collision in an around the vehicle environment and analyze the collected data to have the conclusion regarding the collision while simultaneously transmitting the data over the wireless network. The Evidence Collection System is vehicle based device which collect the data like speed, engine temperature, acceleration, GPS position, wiper movement, and time. This data can be used to investigate the crime, rescue operation and insurance claims. This data then transmitted to the database server so that web application can be able to access this information at different places like Police station, Insurance Company.

7. Divyashree K, Likhithesh M D, Arpitha M,MadanRaj K S,Raghu S,Vinay Kumar S B(2015) explains that the Car black box is a device used to record the information's such as engine temperature, presence of obstacle, alcohol content and exact location of the accident about the vehicle. Along with this we are using Smartphone to get the snap shots which are related to accidents and finally send this information along with the snaps to police sever.

8. Ananthakrishnan V.K, R. Vignesh Kumar, C. Jagadeesh Vikram, C. Thamotharan(2015) says that in order to record informational data, such as engine, vehicle speed and its temperature, etc. to revolutionize the field of motor vehicle accident investigation. It can be also used for vehicle mapping and accident alert with the help of GPS and GSM technology. It records the data for safety and it performs the logical operations.

9. Rajashri R. Lokhande, Sachin P. Gawate (2015) explains that the Wireless black box using MEMS accelerometer and GPS tracking system is developed for monitor the accident. Using MEMS wireless device will send mobile phone short massage indicating the position of vehicle by GPS system to family members, nearest police station and hospitals. The emergency medical service (EMS) is provided to the driver.

IV. EXISTING SYSTEM

Modern vehicles use a number of onboard computers to control driving systems, including acceleration, braking and airbag deployment. The computers are connected to sensors throughout the vehicle and send the sensor data to EDR (Event Data Recorder aka Vehicle Black Box). But these EDRs have limitation, for example, in the recently alleged unintended-acceleration incidents involving Toyota, the expert witness said that EDR itself went wrong during the crash event and as a result the data that was stored is not good enough to figure out whether the car or the driver is to blame. Some of the standalone Digital Video/Audio Recorders that are currently in the market are used primarily for security purpose and thus are not going to help to analyze a crash event.

V. GPS

The Global Positioning System (GPS) is a location system based on a constellation of about 24 satellites orbiting the earth at altitudes of approximately 11,000 miles. GPS was developed by the United States Department of Defense (DOD), for its tremendous application as a military locating utility. The DOD's investment in GPS is immense. GPS has proven to be a useful tool in non-military mapping applications as well. The smart antenna can track upto 66 satellites at a time.

Fast time to first fix Superior sensitivity, and Low power. Less than 10m Accuracy.57600bps UART interface. Up to 10Hz update rate.Built-in micro battery to preserve system data for rapid satellite acquisition.LED indicator for fix or no fix.GPS satellites are orbited high enough to avoid the problems associated with land based systems, yet can provide accurate positioning 24 hours a day, anywhere in the world. Uncorrected positions determined from GPS satellite signals produce accuracies in the range of 50 to 100 meters.Today, many industries are leveraging off the DOD's massive undertaking. As GPS units are becoming smaller and less expensive, there are an expanding number of applications for GPS. In transportation applications, GPS assists pilots and driversin pinpointing their locations and avoiding collisions.

VI. MAGNETOMETER

Magnetometers, which measure magnetic fields, are distinct from metal detectors, which detect hidden metals by their conductivity. When used for detecting metals, a magnetometer can detect only magnetic (ferrous) metals, but can detect such metals buried much deeper than a metal detector. Magnetometers are capable of detecting large objects like cars at tens of meters, while a metal detector's range is unlikely to exceed 2 meters. The magnetometer is based on the idea that the magnetic flux moving through a coil depends on the orientation of the with respect to the magnetic field lines of the earth.

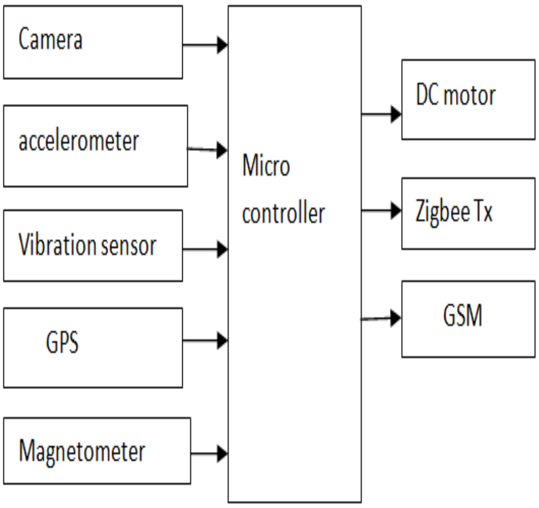


FIG1.Block diagram-Transmitter

The above block diagram transmitter side contains Zigbee used for transforming the data. Camera is used to capture the scenarios of car. Magnetometer is used to find the attitude and longitude.GSM is used to send notification.

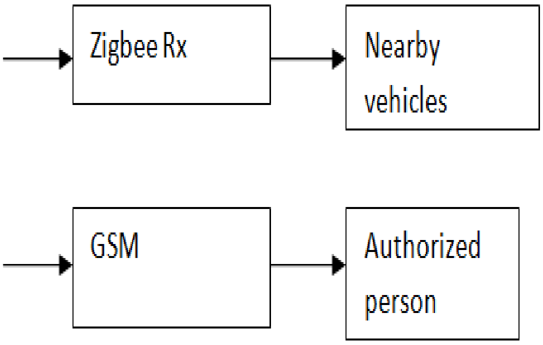


FIG 2.Block diagram-Receiver

VII. CONCLUSION

The project Recorders and standalone Digital Video/Audio recorders. The E-Crashcorder is integrated within the Electronic Control Unit. Responsible for the airbag control and deployment and stores the status of vehicle gathered from different sensors. is the combination of all the advantages of previous Black Boxes, Event Data Recorders. The system that we can track the car location just by sending the mobile SMS.

REFERENCES

[1] Joe T.Correia, KenA.Illiadis,S.Mccarron"Utilizing m Automative Event Data Recorder ".

[2] Anoop Mathew, Joseph Kuncheria, Yadukrishnan S, Gifty Raju, Haritha Chandrasekhar "Car Black Box" International Journal of Innovative Science and Modern Engineering (IJISME) ISSN: 2319-6386, Volume-2 Issue-11, October 2014.

[3] Mohamad-Hoseyn Sigari 1, Muhammad Reza Pourshahabi"A Review on Driver Face Monitoring Systems for Fatigue and Distraction Detection" International Journal of Advanced Science and Technology Vol.64(2014),pp.73100.

[4] Mr. Kishor Rane ,Mr. Rahul Tichkule ,Mr. Mohit Shinde" Online Black Box System for Cars "International Journal of Engineering Science Invention ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726.

[5] Ramchandra Patil, Shivaraj Hublikar "Design and Implementation of Car Black Box with Collision Avoidance System using ARM" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-4, Issue-3, August 2014.

[6] M.Tote kanapurkar Evidence collection System for car using Embedded system and.NET Framework"2014.

[7] Divyashree K, Likhithesh M D, Arpitha M,MadanRaj K S,Raghu S,Vinay Kumar S B" Proof collection from car black box using smart phone for accident detection" ISSN : 2248-9622, Vol. 5, Issue 5, (Part -5) May 2015, pp.16-20

[8] Krishnan V.K,R.Vignesh Kumar, C.jagadeesh Vikram,"Design and Fabrication of Black box for Automobiles" 2015.

[9] Rajashri R. Lokhande1, Sachin P. Gawate2"Design and Implementation of vehicle Black Box For Driver Assistance andAlert"IOSR Journal of Computer Science (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727.

ELECTRONIC HAND GLOVE GESTURE TO VOICE RECOGNIZATION USING MUTE AND BLIND

V. Rajalakshmi[#1]. Mr.N.Vasudevan[*2] Dr.Rajinigrinath[*3] Mr.S.Praveen kumar[*4]

[#1]PG Student, Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai.
*[*2]Assistant Professor, Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai.*
*[*3]Head of the Dept, Department of Computer Science and Engineering Anand institute of higher technology, Chennai.*
*[*4]Assistant Professor, Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai.*

Abstract- **In the past, hand postures and gestures as a mechanism for interaction with computers, describing both the various techniques for performing accurate recognition and the technological aspects inherent to posture- and gesture-based interaction. First, the technological requirements and limitations for using hand postures and gestures are described by discussing both glove-based and vision-based recognition systems along with advantages and disadvantages of each. Second, the various types of techniques used in recognizing hand postures and gestures are compared and contrasted. Third, the applications that have used hand posture and gesture interfacesare examined.Then it will help the deaf person to communicate with others by typing text on LCD screen through hand gestures. The text is converted into speech so that the blind person could hear and communicate. It difficult for a novice to determine whether and how well a particular glove suits a particular cameras to capture the sequence of images. Although, the latter is a more natural approach, it is usually application.**

Index Terms- **Feature extraction, pattern recognition, sensor gloves, sign language recognition.**

I. INTRODUCTION

The series of gestures such as hand movements and facial expressions indicating words are referred to as sign language. It is a form of communication used mostly by people with impaired hearing. Sign language recognition systems are used to convert sign language into text or speech to enable communication with peo-ple who do not know these gestures. Usually, the focus of these systems is to recognize hand configurations including position, orientation, and movements. Generally, there are three levels of sign language recognition: finger spelling (alphabets), iso-lated words, and continuous gesturing (sentences). Accordingly, these configurations are captured to determine their correspond-ing meanings, using two approaches: sensor-based and vision-based. While the former entails wearable devices to capture gestures, it is usually simpler and more accurate.

On the other hand, vision-based approaches utilize especially of the one describing how gloves were applied for different uses, can then help this matching process, at the same time highlighting practical issues that may arise during it. While aiming at the novice readers who plan to be esessentially“users” of sensorized gloves, this paper can, we hope, still inspire the specialists, the “producers” or designers of new devices. Inspiration may not necessarily spur from the specialized literature these readers might be more familiar with. Instead, literature these readers might be more familiar with. Instead, by glancing outside their area of expertise, they may discover common threads between their research and research in other fields.Sensor-based recognition systems depend on instrumented gloves to acquire the gesture’s information. In general, equipped sensors measure information related to the shape, orientation, movement, and location of the hand. For SL, several isolated word recognition systems were proposed using sensor gloves. Using Power Gloves, Mohandes and Buraiky developed a gesture-based SL recognition system using a Support Vector Machine classifier for a dataset of 120 words. In Cyber-Gloves and two hand-tracking devices were used to collect a dataset of 100 two-handed SL signs with 20 samples per ges-ture. The reported accuracy is 99.6%. Using the same dataset, Mohandes and Deriche separated the features obtained from the CyberGlove and the hand-tracking system to test the effect of fusing their features at different levels.

The requirement of using hand trackers makes Cyberglove a nonideal option for sign language recognition. DG5-VHand Gloves1 are better suited for this application because they contain flex sensors and a 3-D accelerometer. In Assaleh et al.proposed a low-complexity word-based classification system based on a method of accumulated differences to eliminate the temporal dependence in SL data. The system was designed for isolated word recognition using two DG5-VHand data gloves. The systems release the users from wearing gloves. A survey of existing SL recognition systems is in recognition rates were 92.5% and 95.3% for user-independent and user-dependent modes, respectively. Leap motion controllers for finger and hand motion detection have been used in SL recognition.

Although hand postures and gestures are often considered identical, there are distinctions between them. A hand posture is defined as a static movement. For example, making a fist and holding it in a certain position is considered a posture. With a simple posture, each of the fingers is either extended or flexed but not in between;

For example a fist, pointing, and thumb are up. With a complex posture, the fingers can be bent at angles other than zero or ninety degrees. Complex postures include various forms of pinching, the “okay” sign and many of the postures used in finger spelling.

For example, Kong and Ranganath proposed a segment-based probabilistic method for continuous American Sign Language recognition. They used one Cyberglove with three Polhemus trackers to form a dataset of 74 Single handled sentencses 107 vacabulary.Their Signer inndependent system achieved a recall rate of 86.6% and 89.9 % precision. Gao et al. in developed a user-independent Chinese sign language (CSL) recognition system for both isolated and continuous signs. Two Cybergloves with 18 sensors each and three Polhemus 3SPACE-position trackers were used as input devices. Using this model an accuracy of 82.9% was achieved for 5113 isolated signs. With a dataset of 400 continuous CSL sentences collected from three different signers, CSL recognition system was proposed by Zhang et al. in They used one 3-D accelerometer (ACC) and five electromyographic (EMG) sensors. The authors reported a 93.1% word accuracy and 72.5% sentence accuracy for 72 single-handed words forming 40 sentences and performed by two right handed signer.

In this paper we propose a system for glove-based continuous SL recognition using statistical feature extraction and a modified version of the KNN algorithm. We collect and label a dataset similar to that reported in which was compiled for a vision-based system.

The remainder of this paper is organized as follows. Section introduces the glove-based continuous SL dataset. Section III presents the proposed literature surveying and feature extraction techniques. In Section IV, we discuss the proposed classification approach that is based on KNN. The experimental methods and flex sensor circuit are in Section V, and the experimental results are in Section VI. Section VII concludes the work.

II. MOTIVATION OF RESEARCH

Motivation of this research is to enable communication between blind, deaf and mute people using Electronic Hand-Gloves.

- Check power management using LCD.
- Have low cost with high energy implemented?

III. LITERATURE SURVEY

[1].Zimmerman, Thomas G. "Optical flex sensor." (1985.) says that optical flex sensor is provided and consists of a flexible tube having two ends, a reflective interior wall within the flexible tube and a light source placed within one end of the flexible tube and a photosensitive detector placed within the other end of the flexible tube to detect a combination of direct light rays and reflected rays when the flexible tube is bent.

[2].Watson, Richard. *A survey of gesture recognition techniques*.Trinity College Dublin, Department of Computer Science,(1993)explains that use of hand postures and gestures as a mechanism for inter-action with computers, describing both the various techniques for performing accurate recognition and the technological aspects inherent to posture- and gesture-based interaction. First, the technological requirements and limitations for using hand postures and gestures are described by discussing both glove-based and vision-based recognition systems along with advantages and disadvantages of each. Second, the various types of techniques used in recognizing hand postures and gestures are compared and contrasted. Third, the applications that have used hand posture and gesture interfaces are examined. The survey concludes with a summary and a discussion of future re-search directions.

[3].Laura Dipietro, Angelo M. Sabatini and Paolo Dario (2008) says a Hand movement data acquisition is used in many engineering applications ranging from the analysis of gestures to the biomedical sciences.Glove-based systems represent one of the most important efforts aimed at acquiring hand movement data. While they have been around for over three decades, they keep attracting the interest of researchers from increasingly diverse fields. This paper surveys such glove systems and their applications. It also analyzes the characteristics of the devices, provides a road map of the evolution of the technology, and discusses limitations of current technology and trends at the frontiers of research.

[4]. Saurabh P. Jain, Abhishek Deshmukh, Abhii Shah, Mahendra Pawar says that Traditional keyboards are not re-configurable as per the need of user. Also use of traditional keyboard in multilingual environment is tricky job. The virtual keyboard we proposed uses only 2D webcam and no other hardware and a sheet of paper with keyboard printed on it. This paper addresses problems with traditional keyboard implementations and describes some unique and efficient techniques to solve these problems.

[5]. Dipietro, Laura, Angelo M. Sabatini, and Paolo Dario.(2008)explains that a cyberphysical construction kit that allows users to create custom robots out of craft material, easily assemble the robots using joint modules and control them using hand gestures. These handcrafted robots are assembled using our modules packaged with actuator, wireless communication and controller electronics. These modules eliminate the need for expertise in electronics and enable a plug and play system that directly encourages users to explore by quick prototyping. We designed a glove embedded with sensors to enable the user to control the robots using hand gestures. We present different usage scenarios to demonstrate the system's versatility such as vehicular robot, humanoid puppet, robotic arm, and other combinations. This paper describes the ChiroBot system, interaction methods, few sample creations, and proposes possible "play value".

[6]. Jennifer L. Copeland and Dale W. Esliger (2009) explains that the purpose of this study was to define an accelerometer-count cut point for a group of older adults and to then assess the group’s physical activity for 7 days.Participants (N = 38, age 69.7 ± 3.5 yr) completed a laboratory-based calibration with an Actigraph 7164 accelerometer. The cut point defining moderate to vigorous physical activity (MVPA) was 1,041 counts/min. On average, participants obtained 68 min of MVPA per day, although more than 65% of this occurred as sporadic activity. Longer bouts of activity occurred in the morning (6 a.m. to 12 p.m.) more frequently than other times of the day. Almost 14 hr/day were spent in light-intensity activity. This study demonstrates the rich information that accelerometers provide about older adult activity patterns—information that might further our understanding of the relationship between physical activity and healthy aging.

[7].. X. Chen, C. Zhang, D. J. Webb, R. Suo,G. D. Peng,K. Kalli explains that an optical bend sensor based on a Bragg grating written in an eccentric core polymer optical fibre. The grating wavelength shifts are studied as a function of bend curvature and fibre orientation and the device exhibits strong fibre orientation dependence, wide bend curvature range of ± 22.7 m-1 and high bend sensitivity of 63 pm/m-1, which is 80 times higher than the reported sensor based on an offset-FBG in standard single mode silica fibre.

[8].Hildreth, Evan. "Optical flow based tilt sensor”. 2008 says that described for determining a description of motion of a moving mobile camera to determine a user input to

an application. The method may involve capturing a series of images from a moving mobile camera and comparing stationary features present in the series of images. Optical flow analysis may be performed on the series of images to determine a description of motion of the moving mobile camera. Based on the determined motion, a user input to an application may be determined and the application may respond to the user input, for example, by updating a user interface of the application.

IV. CONCLUSION OF LITERATURE SURVEY

The hand gesture glove a clear that the breadth of research in glove devices has expanded and grown over the past three decades. This area of research remains very active and it is evident that technological advances in computing, sensor devices, materials and processing/classification techniques will make the next generation of glove devices cheaper. More powerful, versatile and, we hope, more ubiquitous.The role of software in making glove devices more ubiquitous in our daily lives cannot be overemphasized.

Recent history has shown that when the underlying software is intuitive and seamless, then mass adoption of the device is a consequence (e.g., iPod). We suspect that this moment is not far away for glove devices—the time frame will continue to be shortened as researchers from different areas of academia and industry work toward resolving the technological challenges discussed. The maximum sentence-based classification rate was 98.9%.It is compared with an existing vision-based solution that uses the same dataset. The highest sentence-based classification rate for the reviewed system was 75%. Finally, since the proposed solution is sensor-based then all of the inherent limitations of vision-based systems are overcome.

V. FLEX SENSOR CIRCUIT

Flex Sensor are normally attached to the glove using needle and thread. They require 5Volt input and output between 0 and 5Volt the resistivity varying with the sensor degree of bend and the voltage output change accordingly. The Sensor connect to the device via 3 pin connector(Ground,Live and Output).The device can activate the sensor from sleep mode, enabling them to power down when not in use and great by decrease power consumption.

The Flex Sensor pictured below changes resistance when bent. It will only change resistance in one direction. An unflexed sensor has a resistance of about 10,000 ohms. The Flex Sensor is bent, the resistance increases to 30-40 kilo ohms at 90 degree. The Output from the flex sensor are input to LM258/LM358 amps and used a non inverted style setup to amplify their voltage. The greater degree of bending the lowest the output voltage. The output voltage is determined based on the equation vin*r1(r1+r2) where r1 is the other input resistor to the non-inverting terminal.

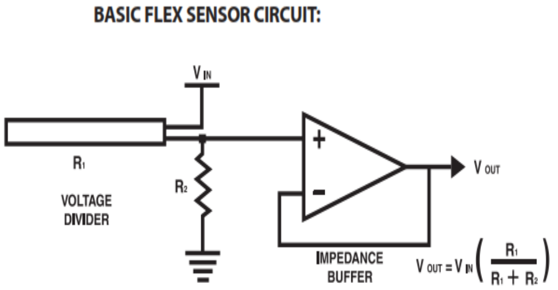

BASIC FLEX SENSOR CIRCUIT:
V IN
R1
VOLTAGE DIVIDER
R2
+
-
V OUT
IMPEDANCE BUFFER
$V_{OUT} = V_{IN}\left(\frac{R_1}{R_1 + R_2}\right)$

Figure 1 Basic Flex Sensor Circuit

Using the voltage divider concept the output voltage is determined and it range from 1.35V to 2.5V. Therfore Micro controller APR is used as the Main Controller in this project. It has built ADC module, which digitize, all analogue signals from the sensors and inbuilt multiplexer for sensor signal selection. It supports both serial and parallel communication facilities.The flex sensor to connect the hand glove is attached to the finger in the point where the motion of axis generates analog signal. Then use analog to digital converter converts analog to digital signal with repills.MOSFET converter is used to give the purified digital signal to the controller and the generating power using LCD display.

VI. CASE STUDY

The integration of piezoelectric energy harvesters allows for an increase of the battery charge through hand movements. From the experimental results (i.e., repetitive opening-closing of the fingers), the total average power generated is 31.9 µW (6.6, 8.5, 8.5 and 8.3 µW for each finger, from 2 to 5, respectively). By considering the power consumption of the optical port (4.25 mW), the operative duty cycle of the system is 133.2. The measurements of power consumption at the rectification-leveling circuit output reveal approximately 11% of additional expenses (i.e., 0.5 mW). Then, by including all of the sources of electric power consumption, the system duty cycle is approximately 146.5. With the reported duty cycle and without using batteries, the light emitter could be active for 30 s per hour.It is suitable for increasing the battery charge and/or reducing the battery size.

The Electronic Hand-Gloves can interact with the machine through the light channel. The commands imposed by the user through hand motion and light switching are processed by the dedicated software and converted to the corresponding logic instructions for the microcontroller. The commands sent by the glove correspond to specific codified instructions associated with hand gestures.

Many different type of machines can be operated by the mentioned microcontroller, just by changing the coding of the underlying software, depending on the parameters to be controlled. After the initial setup of the interface software, the microcontroller can operate the machine.

The voltage generated by the energy harvester has a random shape; the diode bridge provides the first voltage rectification, and the following capacitor levels the voltage at the desired value. The next operational control regulates the charge/discharge of the internal capacitance by allowing the current to flow towards the main battery only when the charge voltage threshold is reached.

The instant voltage level on the capacitor can be measured from the VC port. The curves show the voltage the functioning circuit: the random input voltage charges the capacitor to the voltage level VH; the capacitor discharge starts at the constant output value VOUT. When the discharge of the capacitor reaches the voltage level VL, the output power flow stops. The output voltage (VOUT) is set to 3 V to charge the main battery (Ni-MH rechargeable, 2.4 V, 160 mAh). In the scheme shown in Fig. 8b, the switch on the right side represents the flexible contact made with the conductive fabric.

VII. CONCLUSION

The hand gesture glove a clear that the breadth of research in glove devices has expanded and grown over the past three decades.This area of research remains very active and it is evident that technological advances in computing, sensor devices, materials and processing/classification techniques will make the next generation of glove devices cheaper.more powerful, versatile and, we hope, more ubiquitous.The role of software inmaking glove devices more ubiquitous in our daily lives cannot be overemphasized. Recent history has shown that when the underlying software is intuitive and seamless, then mass adoption of the device is a consequence (e.g., iPod). We suspect that this moment is not far away for glove devices—the time frame will continue to be shortened as researchers from different areas of academia and industry work toward resolving the technological challenges discussed.

The maximum sentence-based classification rate was 98.9%.It is compared with an existing vision-based solution that uses the same dataset. The highest sentence-based classification rate for the reviewed system was 75%. Finally, since the proposed solution is sensor-based then all of the inherent limitations of vision-based systems are overcome.

REFERENCES

[1]. S. Ong and S. Ranganath, “Automatic sign language analysis: A survey and the future beyond lexical meaning,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 27, no. 6, pp. 873–891, Jun. 2005.

[2]. K. Assaleh and M. Al-Rousan, “Recognition of Arabic sign language alphabet using polynomial classifiers,” *EURASIP J. Appl. Signal Process.*, vol. 2005, pp. 2136–2145, Jan. 2005.

[3]. O. Al-Jarrah and F. A. Al-Omari, “Improving gesture recognition in the Arabic sign language using texture analysis,” *Appl. Artif. Intell.*, vol. 21,no. 1, pp. 11–33, 2007.

[4]. T. Shanableh, K. Assaleh, and M. Al-Rousan, “Spatio-temporal feature extraction techniques for isolated gesture recognition in Arabic sign language,” *IEEE Trans. Syst., Man, Cybern., Part B, Cybern.*, vol. 37, no. 3, pp. 641–650, Jun. 2007.

[5]. T. Shanableh and K. Assaleh, “User-independent recognition of Arabic sign language for facilitating communication with the deaf community,” *Digital Signal Process.*, vol. 21, no. 4, pp. 535–542, Jul. 2011.

[6]. T. Shanableh and K. Assaleh, “Telescopic vector composition and polar accumulated motion residuals for feature extraction in Arabic sign language recognition,” *J. Image Video Process.*, vol. 2007, no. 2, pp. 9–9,2007.

[7]. K. Assaleh, T. Shanableh, M. Fanaswala, F. Amin, and H. Bajaj, “Continuous Arabic sign language recognition in user dependent mode,” *J. Intell. Learning Syst. Appl.*, vol. 2, no. 1, pp. 19–27, 2010.

[8]. M. Mohandes and S. Buraiky, “Automation of the Arabic sign language recognition using the Power Glove,” *ICGST Int. J. Artif. Intell. Mach. Learning*, vol. 7, no. 1, pp. 41–46, 2007.

[9]. M. A. Mohandes, “Recognition of two-handed Arabic signs using the CyberGlove,” *Arabian J. Sci. Eng.*, vol. 38, no. 3, pp. 669–677, 2013.

WARNING OF ROAD HAZARD USING WIRELESS BIKE AUTHENTICATION HELMET WITH THE TRAFFIC ADAPTIVE MP3 PLAYBACK

S.SAVITHA[*1],Mrs.A.RUTH TABITA[*2], Mrs.M.MASHEWARI [*3], Mr.D.RAJINIGIRINATH[#4]

[*1]*P.G Student, M.E CSE, Anand institute of higher technology, Chennai, T.N, India.*
[#2,3]*Asst.prof, Dept of CSE, Anand institute of higher technology, Chennai, T.N, India*
[#4]*Head of the Dept,Dept of CSE,Anand institute of higher technology, Chennai, T.N, India*

ssavitha.keerthir@gmail.com

Abstract--**In India still most of the people prefer two wheelers compared to other form of vehicle due to simplicity and its low cost. Oneimportant problem is bike riders suffer from inadequate roads and bad driving conditions. Other important problem with bikers is that most of the time they don't like to wear helmet which could be fatal when accidents happen. Two wheelers in everyone's life play vital role, moreover the safety is considered to be primary of all. According to some statistics 50% of accident occurs due to bad conditions of road and not wearing helmet. To avoid accidents and to encourage people to wear helmet a project is to be introduced that includes smart interactive robotic helmet with features like road hazard warning, wireless bike authentication and traffic adaptive mp3 playback. This helmet will warn the rider when road hazard is ahead, helmet will also communicate with rider if he is not wearing it and will perform wireless bike authentication that act as prevention from theft. It will also adjust the volume of the speakers automatically while rider is listening to music as a safety precaution. Since in India the usage of two wheelers is more compared to four wheelers, it requires more attention as far as safety is concerned.**

Keywords - **Road hazard warning, bike authentication, ARM cortex, audio decoder.**

I. INTRODUCTION

People prefer motorcycles over car as it is much cheaper to run, easier to repair, easier to park and flexible in traffic. In India more than 37 million people are using two wheelers. Since usage is high accident percentage of two wheelers are also high compared to four wheelers. Motorcycles have high rate of fatal accidents than automobiles or trucks and buses. Nearly 600 people lost their lives in road accidents last year. One third of all those who died in road accidents could have survived had they worn a helmet. Studies shows that usage of helmet can save accident death by 30 to 40 percent.The rate at which number of two wheelers in India is rising are 20 times the rate at which human population is growing. In such scenario fatalities are only going to raise if things do not change fast.

The risk of death is 2.5 times more among riders not wearing a helmet compared with those wearing a helmet.According to statistics serious head injuries can happen even in low speeds. Ninety percent of head injury cases are due to road traffic accidents, about 72 percent are youngsters in the age group of 18 to 40.At least three young men using two wheelers die every ten minutes in India due to head injury.

For a young Indian chance of being killed or disabled by road traffic injury is higher than HIV, heart attack or cancer. Head injuries have acquired the status of a public health problem. These scenarios grabbed my interest over this paper in order to ensure safe bike riding.Process is started and stopped with a simple push button fitted on the helmet that runs on a microphone. For instance, if rider runs into a blind spot at an intersection path hole in the road, he can activate the microphone by pressing this button and then record bad intersection or dangerous hole.

With GPS technology installed helmet will then detect when the rider is travelling near those spots another day and turns on the recorded audio. Of course the rider could also record anything that he is interested like favorite shops, food malls to remind him again. The recorded audio files will be available in the dashboard graphical display and the rider has the option to delete it at any time.

The helmet unit has wireless communication capability so that bicyclist would be warned when the bike is started without wearing helmet. The rider should bring the helmet within 100cm of dash board for helmet presence authentication. Although this is simple authentication it could act like an object password and gives additional protection from theft. The dashboard will show the list of mp3 files stored in the memory card and will play the file that is selected by the rider.When detecting important traffic sounds like fire siren or horn sound it mutes music automatically and when there is no traffic sound the music volume will gradually raise.

Thus the helmet establishes communication between rider and the environment and creates a kind of virtual city or augmented reality city that is used to improve the rider comfort and safety.The rider location is tracked using GPS modem. The generated voice is recorded as mp3 format files in a 2GB Micro-SD memory card. The voice files are decoded and played with the help of mp3 audio codec chip. Helmet communicates with bike unit using IEEE 802.15.4 wireless network protocol.

The bike unit has a graphics LCD and a keypad as its main user interface. The aim of the project is all about designing a Smart Interactive Helmet that can record speech through built-in microphones, and GPS warns the wearer of hazards on a given route. It also can play music and when detecting important traffic sounds like a fire siren or horn sound it mutes music automatically. It has a wireless communication installed so a bicyclist would be warned when he starts his bike without wearing a helmet and can operate the smart helmet from the bike dashboard.

II. SYSTEM OVERVIEW

Helmet unit is capable of recording human speech using the built-in microphones and saves it as audio files. The recordingThe helmet has a built-in microphone near the mouth to record voice and an external second microphone to monitor the traffic noise. The helmet unit and bike unit has LPC1313, a 32-bit ARM cortex-M3 microcontroller from NxP semiconductors that controls everything from playing music on to recording voice commands and communicating with bike unit.

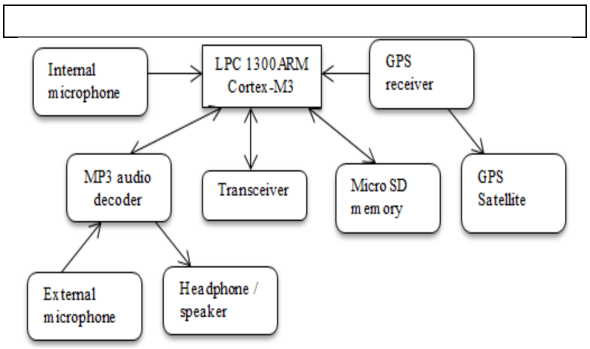


Figure 1: Block diagram

III. BLOCK DESCRIPTION

3.1 Helmet unit

Robotic Helmet unit includes head phone/speaker, satellites, MP3 audio decoder, LPC 1300, ARM Cortex-M3, **3**GPS receiver, IEEE 802.15.4/transceiver, micro SD/memory and external microphone. Head phone acts as a speaker to hear recorded voice and mp3 songs.Microphone is used to record voice or commands given by rider with the help of push button switch provided in the helmet. GPS receiver is used to receive the location of the rider through GPS satellites. IEEE 802.15.4 helps in communicating with bike dashboard unit. ARM cortex-M3 controls everything and external microphone is used to monitor traffic sounds.Bike Dashboard unit includes Graphics LCD, IEEE 802.15.4/transceiver, LPC1300, ARM Cortex- M3 and keypad. Graphics LCD is use for display purpose. It displays menu. ARM Cortex controls every function. Transceiver is used for communicating with robotic helmet unit. Keypad is used for providing input.

IV. HARDWARE DESCRIPTION

4.1 ARM Cortex- M3

The cortex-M3 processor is the first ARM processor based on the ARMv7-M architecture and has been specifically designed to achieve high system performance in power and cost sensitive embedded applications.

The recorded audio files will be available in the dashboard graphical display and rider has the option to delete it at any time. Thus helmet will then detect when the rider is travelling near those same spots another day and trun on the recorded audio.

It has a hierarchical structure. It integrates the central processor core with advanced system peripherals to enable integrated capabilities like interrupt control, memory protection, system debug and trace.These peripherals are highly configurable to allow the cortex-M3 core and the integrated components have been specifically designed to meet the requirements of minimal memory implementation, reduced pin count and low power consumption.The central cortex-M3 core is based on the Harvard architecture characterized by separate buses for instructions and data. By being able to read both instruction and data from memory at the same time, the cortex-M3 processor can perform many operations in parallel, speeding application execution. The core pipeline has three stages: instruction fetch, instruction decodes and instruction execute.

When a branch instruction is encountered, the decode stage also includes a speculative instruction fetch that lead to faster execution. The processor fetches the bank destination instruction during the decode stage itself. Later, during the execute stage, the branch is resolved and it is known which instruction is to be executed next.If the branch is not to be taken, the next sequential instruction is already available. If the branch is to be taken, the branch instruction is made available at the same time as the decision is made restricting idle time to just one cycle.Performance of cortex-M3 is high compared to PIC18, PIC24, dsPIC and Cortex-M0. High performance often 10x better than the fastest 8051 and 2-3x better than 16-bit MCU.

Performance is better even at same or lower clock speeds. And it provides excellent Dhrystone benchmark performance of1.25 DMIPS/MHZ. It also implements the new thumb-2 instruction set architecture, helping it to be 70% more efficient per MHZ than an ARM7TDMI-S processor executing thumb instructions and 35% more efficient than the ARM7TDMI-S processor executing ARM instructions for the Dhrystone benchmark.Energy efficiency of Cortex-M3 is much better compared to other types.

It helps to squeeze more functionality out of precious battery life and enables to meet the increasing demands for low energy products. It has smallest code size of any microcontroller. Reducing code size is key to squeezing application code into the minimum amount of flash which is easily achieved in cortex-M3.

4.2 LPC1300

LPC1300 microcontroller family is based on the ARM Cortex-M3 architecture for embedded applications featuring a high level of support block integration and low power consumption. The peripheral complement of the LPC1300 series includes up to 32 KB of flash memory, up to 8 KB of data memory, USB device interface, UART with fractional baud rate generation, SSP controller with FIFO and multi-protocol abilities, SPI interface, I2C bus interface supporting full I2C bus specification, 8 channel 10-bit ADC, 4 general purpose timer/PWMs, and up to 40 general purpose I/O pins On-chip.

ROM is also present which contains in-system programming capability supporting UART and USB flash programming as well as APIs for user code. The flash API implements a simple interface to the on-board flash programming functionality and allows entry to ISP mode at any time. The USB API supports development of human interface devices and mass storage class devices without requiring driver code to be written by the customer or stored in flash. It runs at frequencies up to 72 MHZ and built-in Nested vector interrupt controller. Single power supply (2.0 V to 3.6 V). GPIO pins can be used as edge and level sensitive interrupt sources.

4.3 MP3Audio decoder

It is device or program capable of coding or decoding digital data stream. It can decode multiple formats such as MP3, AAC, WMA, FLAC, WAV, and MIDI. It uses SPI protocol to interface with LPC1300. It is used to control volume, bass and treble.

Its features includes low power operation, high quality on-chip stereo DAC, zero cross detection for smooth volume change, stereo earphone driver capable of driving a 30-ohm load, quiet power on and off, 16.5 KB on-chip RAM for user code and data.

4.4 Graphics LCD

Graphics LCD used in this project is PCD8544. It is a low power CMOS LCD controller/driver which is designed todrive a graphic display of 48 rows and 84 columns. All necessary functions for display are available in single chip generation of LCD supply and bias voltage that results in a minimum of external components and low power consumption. PCD8544 is manufactured in n-well CMOSCAN controller MCP2515. Logic supply voltage range VDD to VSS is 2.7 to 3.3V. Display supply voltage range VLCD to VSS is 6.0 to 8.5V with LCD voltage internally generated and 6.0 to 9.0V with LCD voltage externally supplied.

4.5 TRANSCEIVER

IEEE standard 802.15.4 intends to offer the fundamental lower network layers of a type of wireless personal area network which focuses on low cost, low speed ubiquitous communication between devices. The basic framework conceives a 10 meter communication range with transfer rate of 250 kb/s. Tradeoffs are possible to favour more requirements through the definition of not one, but several physical layers. Lower transfer rates of 20 and 40 kb/s were initially defined with 100kb/s rate being added in the current revision. Even lower rates can be considered with the resulting effect on power consumption.

The main identifying feature of IEEE 802.15.4 among WPANs is the importance of achieving extremely low manufacturing and operation costs and technological simplicity without sacrificing flexibility or generality. Devices also include power management functions such as link quality and energy detection.

4.6 Measure of frequency range

An ADC is defined by the range of frequencies it can measure and how accurately it can measure a signal relative to the noise it introduces. The actual bandwidth of an ADC is characterized primarily by its sampling rate and to a lesser extent by how it handles errors such as aliasing. The dynamic range of an ADC is influenced by many factors including the resolution, linearity, accuracy and jitter. The dynamic range of an ADC is often summarized in terms of its effective number of bits. An ideal ADC has an effective number of bits equal to its resolution. In this project it is used to detect the important traffic sounds like traffic horn, fire siren Through External Microphone And Mute The Volume of mp3 so that rider can hear those important traffic sounds and can be cautious.

V. SOFTWARE TOOL

5.1 LPCXpresso IDE

The LPCXpresso IDE is a highly integrated software development environment for NXP's LPC microcontrollers. It includes all the tools necessary to develop high quality software solutions in a timely and cost effective manner. LPCXpresso is based on eclipse and has many enhancements to simplify development with NXP LPC microcontrollers. It also features the industry standard GNU tool chain with a choice of a proprietary optimized c library. It supports NXP's ARM based LPC microcontrollers. The platform is comprised of a simplified Eclipse based IDE and low cost target boards which include an attached JTAG debugger. Features of LPCXpresso are eclipsed based IDE, GNU compiler, linker and libraries, enhanced GDB debugger, supports LPC link programmer and debugger, complete tool chain for LPC1000 series of Cortex-M, developed by NXP semiconductors and code red technologies.

VI. MERITS

The project offers protection from inadequate roads and bad driving conditions that is common in countries like India. The device also allows the rider to record any spot of interest like their favorite shops, food malls to remind him on the road. Large on board memory to store voice files recorded. Ability to delete the previously recorded voice files at a later time which is useful when the hazard has been removed. Smart wireless bike authentication feature acts like a password which is also useful to protect the vehicle from theft. All the units are powered by a 32 bit ARM Cortex-M3 microcontroller which is low cost, low power and provides superior performances compared to available 8, 16 and 32 bit offerings from different vendors.

VII. RESULT

Bike engine starts only when helmet is brought near to bike dashboard unit. The condition is – helmet: present = engine on and helmet: absent = engine : off. Hazard warning information is passed to rider when he is at distance of 10 meters from the hazard to alert him. The volume of MP3 playback is automatically adjusted to mute, when important traffic sounds are detected.

VIII. CONCLUSION

Helmet for road hazard warning is designed with wireless bike authentication and traffic adaptive mp3 playback. The main aim of this project is to encourage people to wear helmet and to prevent road accidents, which is achieved. Thus road accidents can be prevented to some extent and safety of bike riders is ensured.

REFERENCES

[1] M. Akbacak and J. H. L. Hansen, "Environmental sniffing: Noiseknowledge estimation for robust speech systems," IEEE Trans. Audio,Speech, Lang. Process., vol. 15, no. 2, pp. 465–477, 2007.

[2] N. Krishnamurthy and J.H. L. Hansen, "Environment dependent noisetracking for speech enhancement," Int. J. Speech Technol., vol. 16, no.3, pp. 303–312, 2013.

[3] M. Brandstein and D. Ward, Microphone Arrays: Signal ProcessingTechniques and Applications. Berlin, Germany: Springer Verlag,2001.

[4] A. K. Nabelek and J. M. Pickett, "Monaural and binaural speech perceptionthrough hearing aids under noise and reverberationwithnormalan hearing-impaired listeners," J. Speech Hearing Res., vol. 17, no.4, pp. 724–739, 1974.

[5] S. Gannot and M. Moonen, "Subspace methods for multimicrophonespeechdereverberation," EURASIP J. Appl. Signal Process., vol. 11,pp. 1074–1090, 2003.

[6] E. A. P. Habets, S. Gannot, I. Cohen, and P. Sommen, "Joint dereverberation and residual echo suppression of speech signals in noisy environments,"IEEE Trans. Audio, Speech, Lang. Process., vol. 16, no.8, pp. 1433–1451, Oct. 2008.

[7] S. O. Sadjadi and J.H. L. Hansen, "Blind spectral weighting for robustspeaker identification under reverberation mismatch," IEEE Trans.Audio, Speech, Lang. Process., vol. 22, no. 5, pp. 935–943, 2014.

[8] N. Yousefian and P. C. Loizou, "A dual-microphone algorithm that cancope with competing-talker scenarios," IEEE Trans. Audio, Speech,Lng. Process., vol. 21, no. 1, pp. 145–155, 2013.

SECURE INFORMATION TRANSFER FOR NFC APPLICATIONS

Ms.S.Swathilakshmi[#1], Mr D.Anand Joseph Daniel[*2],Mr S.Praveen Kumar[*3],Mr.D.Rajini Girinath[*4]

[#1]PG Student,Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai.
*[*2,*3]Assistant Professor,Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai.*
*[*4]Professor,Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai.*

sriswathilakshmi10@gmail.com.

***Abstract* - NFC (Near field Communication) is a short-range wireless communication technology whose technology distance is around 4 inches, and it operates in the 13.56MHz frequency band at a speed of 106Kbps to 424Kbps. The combination of NFC with smart devices resulted in widening the range of NFC, which includes data exchange, service discovery, connection, e-payment, and ticketing. It is expected to replace credit cards in electronic payment, especially. Malicious internal attackers can create profiles of users through the acquisition of public keys of other users in the process of key agreement. If NFC is used in e-payment in this way, the privacy of users can be infringed through profiles created by attackers. The proposed methods provide conditional privacy in which the identity of users can be verified by the OTP (One Time Password) to resolve disputes when necessary.**

***IndexTerms* — NFCsecurity, Pseudonym, Unlinkability, Conditional privacy protection.**

I. INTRODUCTION

NFC(Near Field Communication) is a short range high frequency wireless communication technology. NFC is mainly aimed for mobile or handheld devices.A radio communication is established by touching the two phones or keeping them in a proximity of a few centimeters (up to 10 cm) .It allows for simplified transactions, data exchange, and wireless connections between two devices. Allows communication between Two powered (active) devices Powered and non self-powered (passive) devices. In the active NFC mode of communication, both devices generate an RF signal on which the data is carried.

In this passive mode of communication, only one NFC device generates an RF field. The second passive device which is the target uses a technique called load modulation to transfer data back to the primary device or initiator. NFC is an extension of Radio frequency identification (RFID) technology that combines the interface of a smartcard and a reader into a single device. This allow two-way communication between endpoints, where earlier systems were one-way only. Malicious internal attackers can create profiles of users through the acquisition of public keys of other users in the process of key agreement.

The proposed methods provide conditional privacy in which the identity of users can be verified by the TTP (Trusted Third Party) to resolve disputes when necessary. In addition, the PDU (Protocol Data Unit) for the conditional privacy is proposed . The data used to help a future purchase uses protected PDU of NFC-SEC, and data not wanted to be recorded uses conditional privacy PDU selectively, which makes it possible to remove the connectivity with the existing messages. Near field communication is based on inductive-coupling.

NFC works using magnetic induction between two loop antennas located within each other's 'near field'. NFC use an initiator and a target; the initiator actively generates an RF field that can power a passive target. High convenience to the user, because the data exchange is done by bringing two mobiles together. Reduces cost of electronic issuance .Secure communication. No special software. No manual configuration and settings.No search and pair procedure.

The system has the limitation that it can be operated only with devices under a short range i.e around 10 cm.
The data transfer rate is very less at about 106kbps, 212 kbps and 424kbps. For two devices to communicate using NFC, one device must have an NFC reader/writer and one must have an NFC tag. The tag is essentially an integrated circuit containing data, connected to an antenna, that can read and written by the reader. By 2013, one in five phones will have NFC. The analyst forecasts the gross transaction value of made via NFC will exceed $75bn globally by 2013.

Mobile NFC opens up new opportunities in payment, banking, airline ticketing, online shopping and transport.Most of the crucial standards are already in place, but
implementation are not sufficiently widespread.

The rollout of SCWS would provide a new environment in which to develop, execute and distribute content rich applications from the SIM thereby complementing NFC.Mobile NFC is now finding it’s uses in phone to phone data exchange, ticketing and payment. This will continue to grow as more NFC handsets are available and interoperability issues are addressed.

MuPM method:If user A requests TSM for pseudonyms TSM generates n pseudonyms and transmit it to user A then TSM stores the transmitted pseudonyms and ID of the user A.A Pseudonym composed of public key , private key ID of the TSM and signature of the TSM. SuPM method: if we consider the NFC features in the protocol design process,the protocol can be configured so that it can update pseudonym without the need to communicate with TSM.The communication with the TSM can be used only to keep track of the message constructor. Conditional Privacy PDU:In case information is hidden in all situations , there arises a problem where the personalized service is not provided.In this method users can request services through protected PDU if they want to receive the personalized service.

II. MOTIVATION FOR RESEARCH

The motivation of my research is to increase the security level in NFC based application.

- Check attacks in message transfer.
- How much of performance is increased?
- What is computational time?

III. LITERATURE SURVEY

1.Gabriella Arcese says Among the different hi-tech content domains, the telecommunications industry is one of the most relevant, in particular for the Italian economy. Moreover, Near Field Communication (NFC) represents an example of innovative production and a technological introduction in the telecommunications context. Finally, this work presents the state of art of the improvements to this technology with a deeper focus on NFC technologies applied to the tourism industry. In this way, we have done a case analysis that shows some of the NFC existent applications linked to each stage of the tourism value chain.

2.HoyulChoi says OTP is one of the most powerful authentication methods among them. However, it has some security vulnerabilities,particularly to MITM(Man-in-the-Middle) attack and MITPC/Phone(Man-in-the-PC/Phone) attack. An adversary could know a valid OTP value and be authenticated with this secret information in the presence of those attacks. The scheme is secure against MITM attack and MITPC/Phone attack by using a captcha image, IMSI number embedded in SIM card and limiting available time of an attack.

3. Thomas Plos says in Security-Enabled Near-Field Communication Tag With Flexible Architecture Supporting Asymmetric Cryptography a flexible NFC-tag architecture that provides enhanced security features using symmetric aswell as asymmetric cryptography. As a main contribution,the work described an entire “real-world” RFID system,including all hardware components needed for a practicalchip fabrication. to further analyze our design regarding enhanced implementation attacks, such as side channel analysis and fault attacks. Moreover, we plan to implement additional demo applications to verify the applicability of our tag in different security-related scenarios.

4. Rong Jin says a practical and energy efficient key agreement method for duplex NFC. To deal with inconsistency, the method introduces random shaking on RF waveform. The shaking add randomness to hide the inconsistency. To deal with the impact of Gibbs phenomenon, the method adds guard bits between random bits to prevent the attacker determining the bit from the previous one.

5.Wei Li says in Near-Field Communication Transceiver System Modeling and Analysis Using System C/System C-AMS With the Consideration of Noise Issues. how to model and simulate an NFC reader/card transceiver system working under the passive mode using System C/System C-AMS. System C is good at digital circuit modeling from gate level to system level. System C-AM Scan model linear and nonlinear behaviors of analog circuits in ELN and TDF methods, respectively. All above three modeling methods were shown as examples in this paper. Their combination with the smoothly running interface offered a platform for modeling a whole mixed-signal heterogeneous system within one language.

6. John Devlin says in FPGA-Based Implementation of Multiple Modes in Near Field Inductive Communication Using Frequency Splitting and MIMO Configuration a comprehensive frequency splitting theory in inductive communication systems. We have also demonstrated through a practical hardware design the possibility of multiple mode inductive communication systems using the strength of the flux couplings in inductive communication.An FPGA-based implementation is presented to validate the theory and design.

IV. CONCLUSION OF LITERATURE SURVEY

In NFC online payment application have more attacks in information transfer.The existing mehods solve some issues but it have some lacking. The computional cost and memory storage are increased.The proposed method overcome the attacks and reduce memory management.

V. MODES OF OPERATION

Near field communication is based on inductive-coupling.NFC works using magnetic induction between two loop antennas located within each other's 'near field’. In Active mode, both devices with NFC chip generates an electromagnetic field and exchange data. In Passive mode, there is only one active device and the other uses that field to exchange information.Two NFC enabled devices transfer-ring data in active mode

Fig 1:Active Node

A NFC-enabled mobile phone is paired with a RFID-tagged "smart poster"

Fig 2:Passive Node

VI. SECURE NFC INFORMATION TRANSFER MODEL CONSTRUCTION

The proposed methods provide conditional privacy in which the identity of users can be verified by the OTP to resolve disputes when necessary. By using the proposed method various attacks such as,

1.MIMT
2.Impersonation attack
3.Replay attacks
4.Modification attacks
5.Session key security

Once the key agreement rule is satisfied, it will be acknowledged and it will allow to send the data.If it is not satisfied, the connection with the hacker is found and it will be terminated.It includes the following components.The project consists of ARM 2148 controller and NFC readers. The transmitted node consists of micro-controller and NFC reader. Initially the connection between the devices can be established by using the algorithmic steps. The transmitter node sends the encrypted message to the recipient node.

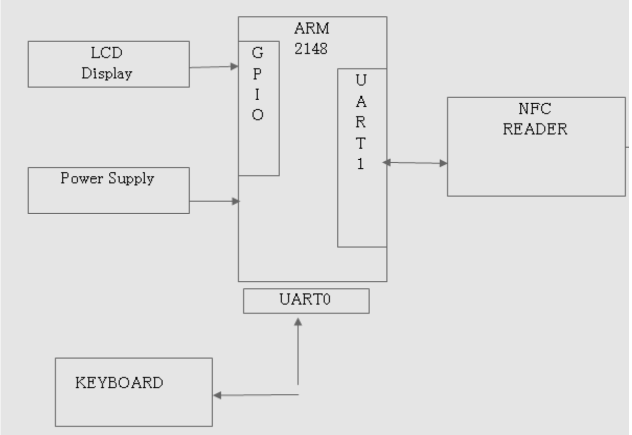


Fig 3:BLOCK DIAGRAM

The smart phone which consists of NFC module is used to encrypt the message to establish the connection. The recipient receives the data and decrypts it and sends it back to the transmitter. If the sender receives the data which matches with its predefined data, the connection will be established. When connection is successfully established, data will be forwarded to the recipient.

If the hackers are pretending as actual recipient, they cannot decrypt the data and never sends the data to the transmitter. So Sender can identify the hacker with a OTP key and terminate the connection with hacker.The method using conditional privacy protocol with OTP method for NFC applications, to avoid several threatening attacks in data communication. This method also overcomes computational cost and time for transfer.

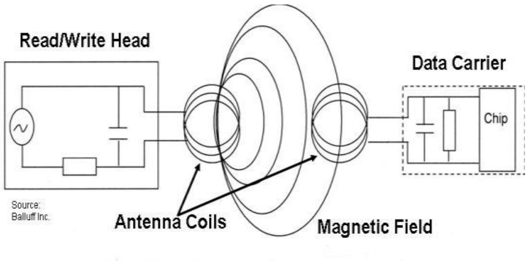
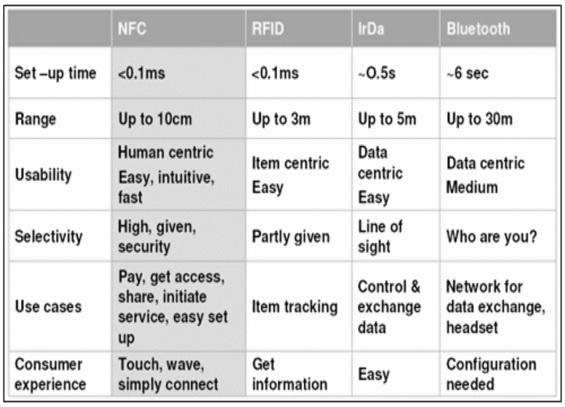


Fig 4:Mechanism in NFC

Proteus developed by Lab center Electronics, is a software with which you can easily generate schematic captures, develop PCB and simulate microprocessor. Proteus provides a powerful working environment. The user can design different electronic circuits with all the necessary components easily accessible from the simple yet effective interface like signal generators, power supply, simple resistor and a different microcontroller or microprocessor.



	NFC	RFID	IrDa	Bluetooth
Set –up time	<0.1ms	<0.1ms	~0.5s	~6 sec
Range	Up to 10cm	Up to 3m	Up to 5m	Up to 30m
Usability	Human centric Easy, intuitive, fast	Item centric Easy	Data centric Easy	Data centric Medium
Selectivity	High, given, security	Partly given	Line of sight	Who are you?
Use cases	Pay, get access, share, initiate service, easy set up	Item tracking	Control & exchange data	Network for data exchange, headset
Consumer experience	Touch, wave, simply connect	Get information	Easy	Configuration needed

TABLE 1: COMPARISON WITH EXISTING TECHNOLOGY

VII. SECURITY REQUIREMENT

In response to the security threats covered in this section, NFC security protocols should satisfy the following properties. In general, the key agreement protocol should be robust to the MITM attack.

□ *Data Confidentiality*: It is required to protect data from unauthorized users.

□ *Data Integrity*: The transmitted data should be identical to the source data.

□ *Unobservability*: The data of specific users should not be distinguished from multiple data.

□ *Unlinkability*: When two data generated by the same user is presented, the connectivity between the two data should not be identified.

□ *Tracability*: It is required to enable to find out who generated the data if a problem occurs.

VIII. CONCLUSION

The OTP method with conditional privacy protocol is used in method.It provide secure information transfer between user and service provider.The OTP concept provide rich security in mobile payment.there is no hole to hackers for steal the information.the conditional privacy method also provide high performance and it reduce storage management.in this method should overcome various types of attacks in NFC application.

REFERENCES

[1] Gartner, "Market Insight: The Outlook on Mobile Payment," Market Analysis and Statistics, May 2010.

[2] Juniper Research, "NFC Mobile Payments & Retail Marketing – Business Models & Forecasts 2012-2017," May 2012.

[3] ISO/IEC 15946-1:2008, "Information technology – Security methods – Cryptographic methods based on elliptic curves – Part 1: General," Apr. 2008.

[4] ISO/IEC 13157-1:2010, "Information technology Telecommunications and information exchange beten systems – NFC Security – Part 1: NFC- SEC NFCIP-1 security service and protocol," ISO/IEC, May 2010.

[5] ISO/IEC 13157-2:2010, "Information technology Telecommunications and information exchange beten systems – NFC Security – Part 2: NFC- SEC cryptography standard using ECDH and AES," ISO/IEC, May 2010.

[6] H. Eun, H. Lee, J. Son, S. Kim, and H. Oh, "Conditional privacy preserving security protocol for NFC applications," IEEE International Conference on Consumer Electronics (ICCE), pp. 380-381, Jan. 2012.

[7] ISO/IEC 18092:2004, "Information technology – Telecommunications and information exchange beten systems – Near field Communication – Interface and Protocol (NFCIP-1)," ISO/IEC, Apr. 2004.

[8] J. Yu, W. Lee, and D.-Z. Du, "Reducing Reader Collision for Mobile RFID," IEEE Transactions on Consumer Electronics, Vol. 57, No. 2, pp. 574-582, May 2011.

[9] E. Haselsteiner and K. Breitfuß, "Security in Near field Communication (NFC) – Strengths and aknesses –," RFIDSec 2006, Jul. 2006.

[10] IEEE Std. 1363-2000, IEEE Standard Specifications for Public-Key Cryptography, Jan. 2000.

[11] G. Calandriello, P. Papadimitratos, J.P. Hubaux, and A. Lioy, Efficient and robust pseudonymous authentication in VANET," Proceedings of the fth ACM international workshop on Vehicular ad hoc networks (VANET 2007), pp. 19-28, 2007.

[12] J.C.M. Teo, L.H. Ngoh, and H. Guo, "An Anonymous DoS-Resistant Password-Based Authentication, Key Exchange and Pseudonym Delivery Protocol for Vehicular Networks," Proceedings of the 2009 International Conference on Advanced Information Networking and Applications (AINA 2009), pp. 675-682, May 2009.

[13] D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler, "Strong and affordable location privacy in VANETs: Identity diffusion using time-slots and swapping," Proceedings of the 2010 IEEE Vehicular Networking Conference (VNC 2010), pp. 174-181, Dec. 2010.

[14] J.-H. Lee, J. Chen, and T. Ernst, "Securing mobile network prefix provisioning for NEMO based vehicular networks," Mathematical and Computer Modelling, vol. 55, No. 1, pp. 170-187, Jan. 2012.

CONTROL AREA NETWORK (CAN) BASED AUTOMATIC CAR THEFT PREVENTION SYSTEM USING MEMS AND GPS

M.kaviya[#1], R.Femila Goldy[*2] ,Mrs.Shanth[*3], Mrs.Ruth tabhitha[*4]

[#2,*3,*4]*PG Student, Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai.*
[#1]*Assistant Professor, Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai.*

kaviyakalai93@gmail.com

***Abstract*- In automobile field, the security and theft prevention are one of the main areas in current scenario. A modern vehicle has been using a key fob from last decade to arm and disarm the vehicles. Once the door of vehicle is close then vehicle is armed and to disarm unlock button of key fob is used. But this system is not more secure. If the key fob is stolen then anyone can unlock the vehicle. Hence for preventing a vehicle from theft a 3D gesture key fob will be used. In 3D gesture key fob one gesture will be made in air to unlock the vehicle. It will contain two different 3D gestures, one is regular gesture for owner of vehicle and another is guest gesture for the guest i.e. for other users and also the finger print authorization and face recognition. In addition for high security data transmission cryptography algorithm will be used and for priority can protocol will be used. This system will also contain features like keypad entry for activate the fuel lines, adjustable motion alarm sensitivity, Fuel cut off and GPS fencing, MEMS sensor and vibration sensor.**

***Keywords*- PIC, MEMS, AES, GPS, GSM, 3D**

I. INTRODUCTION

The rapid rate at which vehicle thefts has been increasing across the world has called for increasing thrust in the field of vehicle anti-theft systems. This particularly assumes significance for expensive vehicles and those who go behind even more expensive cosmetic modifications. The automobile can be stolen for different reasons viz. for resale the vehicle, for commission of crimes or for other reasons. Hence for more security for vehicles, in this paper proposed two security levels are provided.

First, preventing the theft a 3D gesture key fob is made. 3D gesture key fob will disarm or unlock the vehicle by giving secrete 3D gesture in air. In addition if owner of vehicle is agree to give key fob to other then for other user a guest gesture will be used i.e. another gesture for other users. Guest gesture will be activated through SMS by owner of vehicle. Once the gesture is recognized the cryptography (AES) algorithm will be used for secure transmission of data. After the 3D gesture recognition and cryptography algorithm the vehicle will be unlocked.

Once the door of vehicle will open then a password will be sent to owner of vehicle on his/her cell phone for keypad entry. Password will be activated for specific time, within the valid time password should be entered in keypad. If password will match then only vehicle will be ready to use i.e. fuel lines of vehicle will be on otherwise it will be off. Second, we trained the person’s finger print in the database, who wants to open the car door. At that time of opening the door, the finger print is compared with the trained database, if it is

matched the door will open, otherwise it will not open and also. The ignition process of the vehicle is done by face recognition system. Earlier, we stored the person face, who is driving the vehicle.

The face recognition algorithm is used for comparing those faces, when a person start’s the car. The authorized face is matched then only car ignition spark will start. If unknown person is trying to start the vehicle, the ignition spark does not start. Another specification of the project is if any person is trying to damage the vehicle, the vibration sensor is used to sense the values suddenly send the message using the GSM. At the time of password matching or changing any process for user comfortable, the feature can be temporarily disabled and enabled via SMS sent by the owner.

GPS and GSM technologies enable the vehicle owners to track and monitor the vehicle with cell phone at anytime from anywhere. The important enhancement in this feature is its ability to inform the vehicle position even during a GPS outage using dead reckoning method. This is achieved with the help of Inertial Navigation Sensors that consists of a 3- axis MEMS Magnetomete**r** and a 3-axis MEMS Accelerometer which will act as a tilt compensated compass module. When the owner approaches the vehicle, the system automatically verifies the code from remote key and the vehicle emits a head light flash and horn beep to show its presence. This feature is known as car finder and it assists the owner to locate the vehicle in a parking lot where several vehicles are parked.

II. MOTIVATION OF RESEARCH

The motivation of my research is to reduce the theft of the car using finger print and face recognition system.

- How prevent the vehicle from unauthorized person in effective manner?
- How much security will provide to the owner of the car?
- How effectively controlled the vehicle anti-theft system via GSM network?
- How to stop and control the vehicle through SMS?

III. LITERATURE SURVEY

1. Aderibigbe, E.A. (2005) has developed a security system titled: "Design and Construction of a home automation via domestic power line and GSM network which can be used to monitor home appliances in an automated form via the GSM network.

2. Pang-Chieh, W., Ting-Wei, H., Jung-Hsuan, W., & Bo-Chiuan, C. (2007) proposed a security module for the car appliances to avoid stealing and illegal use on other cars. An open structure which includes authentication and encryption by embed a security module in each to protect car appliances was proposed. The identification of components which deals with relevant procedures were also presented in this work. This work was expected to create new business opportunity to the automotive and technology industry.

3. Jayendra1, G., Kumarawadu, S., & Meegahapola, L. (2007) explains about an auto security anti-theft system with an Immobilizer system through the radio frequency identification (RFID) has been presented by which characterizes low hacking rate while ensuring the safety supports of the passengers when the vehicle is hijacked. The active RFID technology has been used for the operation of the immobilizer system whereby three control circuits from the receiving unit which are in the vehicle, namely, ignition circuit, power control unit, and automatic gear changing system, enabling the vehicle speed is brought down to zero in a gradual safe manner. The proposed anti-theft auto security system has been tested under various climate conditions and possible signal instability situations were used to test its reliability. This paper proposes a smart anti-theft car security system, which not only identifies thief but also controls the car.

4. Karl, K., Czeskis, A., Roesner, F., Patel, S., & Kohno, T.(2010) evaluated an experimental security of a modern automobile. This paper shows experimental evaluation issues on a modern automobile and demonstrated the instability of the underlying system structure. It was also carried out on an attacker who is able to penetrate virtually any Electronic Control Unit (ECU) can influence this ability to completely avoid some safety-critical systems. In both the lab and road tests experiments conducted, the ability to oppositional control a broad range of automotive functions and completely ignore driver input including brakes disabling, selectively braking individual wheels on demand, stopping the engine, and so on, were demonstrated. The obtained results showed that it is possible to introduce elementary network security protections into the car.

5. Muhammad, T.Q., Syed, S.Q., Rafia, K., & Khan, M.Y. (2011) developed an embedded system design to control automobile peripherals automatically through voice recognition system. The profile of the authorize user was configured and saved in the system which operates specific settings for the user. Whenever the user wishes to drive the car, system will initiate the personal settings by identifying the users voice which includes the side and rear mirrors setting and seat adjustments. The use of DM642 media processor allows the real time snapshot of the driver to be taken and displayed on the LCD screen with available profile report. The remotely operation of the smart car locked or unlocked was also performed using GSM modem. Some another features such as navigation and tracking of car using GPS module was also incorporated into the system. The latitude and longitude positions were also taken by the system from GPS and real time car location was also display on the PC using GSM modem.

6. Sheikh, I.A., & Sushil, K. (2011) presented Short Message System (SMS) based home security system equipped with motion sensor, smoke detector, temperature sensor, humidity sensor and light sensors. A microprocessor PIC 18F4520 controlled the sensors through the SMS being password. The home security operation has been tested on Vodafone- Fiji network for emergency and feedback responses were obtained for 25 samples. The GSM experiment showed that it takes about 8-10s delay for the security system to reply the relevant civil authorities and occupant in case of emergency. The occupant takes about 18-22s to energize and monitor lights and appliances and then get feedback from home due the network traffic.

7. Montaser, N.R.,& Mohammad, A.A. (2012) explain an efficient automotive security system has been implemented by for anti-theft using an embedded system occupied with GPS and GSM. In this work, the client communicates through this system with vehicles and the vehicles current locations and status are determined using Google Earth. The position of targeted vehicles is tracked by the user on Google Earth. By using GPS locator, the target current location is determined and sent, alongside with various parameters received by vehicles data port, via SMS through GSM networks.

In order to secure the vehicle, the user in a group of users can turn off many vehicle of the fleet if any intruders is noticed to run it by blocking the gas feeding line. This system is considered safe and effective to report emergency situations such as crash reporting or engine failure.

8. Sot, S. (2012) has proposed the use of MMS Based Car Security System for solving issue. This system integrated monitoring and tracking system. SMS and MMS are sent to the owner to initiate fast response most especially when the car is close by. This project focuses on SMS and MMS technology. Whenever intrusion is detected, the SMS and the picture of the intruder are first sent to main user via local GSM/GPRS service provider to user (and/or) police mail ID. The results obtained from the implementation and testing indicated the success in sending MMS to owner within 30 seconds by the prototype. The time taken to receive the SMS and MMS by the owner and police are suitable to take action against intruder. Control commands are also sent to the module by the User while configuring module for master. Only master user can make changes in the module.

9. Kiruthiga, N., & Latha, L. (2014) studied the use of Biometric Approach for Vehicle Security System Using Fingerprint Recognition. In all the areas, an embedded computing technology is used. A competent automotive security system has been implemented using embedded system along with Global System for Mobile (GSM) and Fingerprint Recognition. Literature survey in this work has illustrated vehicle security system using person identification techniques. The survey mainly raised emphasizes on major approaches for automatic person identification, such as fingerprint recognition and various existing vehicle security system. The security system can be implemented using Microcontroller.

10. Patil1, S.V., & Sardeshmukh, M.M. (2014) proposed an embedded control system platform, face recognition system, GPS and MMS (Multimedia Messaging Service) modules by using WLD (Weber Law Descriptor) as an anti-theft smart vehicle security system. The image used is

divided into number of units, then WLD is obtained in different neighborhood and for each unit of an image, WLD histograms are obtained to reserve spatial information. The obtained WLD histograms from different units are concatenated which results in the final set of a face image. Comparison was made between the extracted feature set of face image and that of feature set of database image and real time user identification is presented. The image of an unauthorized person is sent to user via MMS module, if detected unauthorized entry and by sending the image user to the embedded system via MMS module, the embedded security system takes immediate action to stop the vehicle. Also, GPS module is used to track the location of vehicle and prevented vehicle from theft action.

IV. SYSTEM STRUCTURE

In this paper the heart of or system is ARM 7, GPS module and GSM module. GPS module is used to display the coordinates of the vehicle position with help of GSM module as shown in the figure 1, this system built an intelligent security for the vehicle.

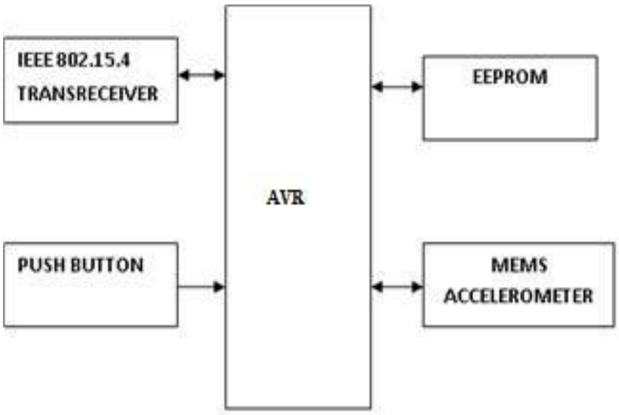


Fig 1: (a) Vehicle Unit & (b) Key Fob Unit

V. SMART GRAVITATIONAL LOCK

The system can be unlock automatically just by pressing lock button from key fob. But to unlock the system a specific gesture is made in hand held wireless key fob.3D gesture is made in air. The air gesture is recognized using a 3-axis MEMS Accelerometer that senses the gravitational force exerted upon it. Without performing the secret gesture stolen key fob cannot be used to enter into the vehicle. The password can be stored in an external non-volatile memory. For gesture recognition process MEMS Accelerometer ADXL335 can be used. The MEMS Accelerometer gives the three dimensions are (x, y, and z) readings of a particular object. The output signals are analog voltages that are proportional to acceleration. The acceleration can measure static and dynamic acceleration. Static acceleration resulting due to tilt and dynamic acceleration are from motion, vibration or shock. The user selects the bandwidth of the accelerometer using the capacitor at the output pins of accelerometer. According to the application the bandwidth can be selected. For X and Y axis the bandwidth range will be 0.5 Hz-1600 Hz, and for Z axis bandwidth range will be 0.5Hz-550Hz.

VI. CRYPTOGRAPHIC KEYLESS ENTRY

In this system Advance Encryption Standard (AES) will be used for secure data transmission. AES, algorithm is a symmetric key cryptography. The AES standard comprises three block ciphers, i.e. AES-128, AES-192 and AES-256. The encryption of AES is carried out in blocks with a fixed block size of 128 bits each. The AES cipher speed can be determined from the number of repetitions rounds in steps which convert the input plain text into the final cipher text. Each round consists of different processing steps, including one that depends on the encryption key. In decryption process a set of reverse rounds are applies to convert the cipher text into the original plain text using same encryption key. The AES-128 algorithm is iterative and consists of 10 rounds. The input is a block of data and the initial key. Each round operates on the intermediate result of the previous round and is a sequence of the four transformations, namely Sub Bytes, Shift Rows, Mix Columns and Add Round-Key. The intermediate result of any step is called the state. The final round is slightly different and the output aft er 10 rounds is the block of encrypted data

A. Encryption Process

The encryption process of AES algorithm consist the following steps:

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

B. Decryption Process

For decryption process following steps is used:

1. Inverse Shift rows
2. Inverse Substitute bytes
3. Inverse Add Round Key
4. Inverse Mix Columns

C. Comparison of AES Block Cipher

Here the comparison of 128 bit key, 192 bit key and 256 bit key is shown in table 1.

TABLE 1: Comparison of AES Block Cipher

Algorithm	*Time Ta ken*	*MB/Sec*
Rijndael (128- bit key)	4.19 6	61.010
Rijndael (192- bit key)	4.81 7	53.145
Rijndael (256- bit key)	5.30 8	48.229

The time taken to 128 bit key is less as compare to other hence in AES 128 bit key block cipher is used. Also 128 bit block cipher key speed is high as compare to other.

VII. CONCLUSION

This project describes an air gesture recognition system by using MEMS accelerometer. The innovative vehicle key is designed in which gesture key from key fob is compared with the stored key to secure opening of the vehicle door. This provides more protection to the vehicle even when the key fob is stolen. Again for the guest a new guest gesture will be given so that the main gesture will be safe. For those adding features like Cryptographic key less entry, key pad entry, Remote fuel cut-off, becomes more secure.

REFERENCES

[1] Aderibigbe, E.A. (2005). "Design and Construction of a home automation via domestic power line and GSM network" Unpublished B.Tech thesis, Department of Electronic and Electrical Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria.

[2] Jayendra1, G., Kumarawadu, S., & Meegahapola, L. "RFID-Based Antitheft Auto Security System with an Immobilizer", Second International Conference on Industrial and Information Systems, ICIIS 2007, 8 11 August 2007, Sri Lanka.

[3] Karl, K., Czeskis, A., Roesner, F., Patel, S., & Kohno, T. "Experimental Security Analysis of a Modern Automobile", Appears in 2010 IEEE Symposium on Security and Privacy.

[4] Kiruthiga, N., & Latha, L. "A Study of Biometric Approach for Vehicle Security System Using Fingerprint Recognition", International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 1, Issue 2, October 2014.

[5] Muhammad, T.Q., Syed, S.Q., Rafia, K., & Khan, M.Y. "Automated Profile Vehicle Using GSM Modem, GPS and Media Processor DM642" Department of Electronic Engineering, Sir Syed University of Engineering & Technology, Karachi, Pakistan, 2009 International Conference on Computer Engineering and Applications IPCSIT vol.2 (2011) (2011) IACSIT Press, Singapore.

[6] Montaser, N.R.,& Mohammad, A.A. "Senior Member", IACSIT, A.A Sharaf, "Intelligent Anti-Theft and Tracking System for Automobiles" International Journal of Machine Learning and Computing, Vol. 2, No. 1, February 2012.

[7] Pang-Chieh, W., Ting-Wei, H., Jung-Hsuan, W., & Bo-Chiuan, C. "A Security Module for Car Appliances" World Academy of Science, Engineering and Technology Vol:1 2007-11-28 . International Science Index Vol:1, No:11, 2007 waset.org/Publication/11397.

[8] Patil1, S.V., & Sardeshmukh, M.M. "Face Recognition by Weber Law Descriptor for Anti-Theft Smart Car Security System." International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 5, May 2014.

[9] Sheikh, I.A., & Sushil, K. "Analysis and Performance of a Low Cost SMS Based Home Security System" School of Engineering and Physics, The University of the South Pacific International Journal of Smart Home Vol. 5, No. 3, July, 2011.

[10] Sot,S."MMS Based Car Security System" International Journal of Electronics and Computer Science Engineering. ISSN-2277-1956.

ANDROID BASED IMAGE TRACKING FOR ENHANCED HOME SECURITY USING ARDUINO MICROCONTROLLER

Gudipudi Sushma#1(ME), Mrs.Mary Joseph*2,Mrs.A.Ruth Tabitha*3, ,Mr.M.B.Prashanth Yokesh*4

Department of Computer Science And Engineering, Anand Institute of higher Technology
Kazhipattur, Chennai, India.

gsushu29@gmail.com

***Abstract-* In recent trends, home surveillance is of keen interest. M2M design was used to communicate to the users when there is an emergency alert like theft. Arduino microcontroller based surveillance improves the efficiency of detecting theft through vibration and PIR sensor. Arduino microcontroller is connected to a USB and converts analog to digital signal, it initiates to capture the image and saves the images in the cloud server to keep track of person involved in the theft. Images are sent to the android users as a trigger alert to deal with intruders.**

***IndexTerms—* Android,Vibration sensor,PIR sensor,cloud server,Arduino microcontroller,Webcam**

I. INTRODUCTION

The need to secure our home, industries and other related properties has been a subject of interest since the days of our fore fathers, Since then, an aggressive develop- -ment in the area of security has exponentially been driven to today's trend.A system cannot have high assurance if it has poor security and requirements. For high assurance,systems will logically include security requirement as well as availability, reliability and robustness requirements.The early-men, in their effort to provide security to their house-hold and properties, used crude measures such as stones, grasses and crude weapons to secure themselves. As the intrusion techniques by intruders outgrows the then security measures and more values added to lives and properties, ore sophisticated mea- -sures were developed to ensure an intruder proof environment, which today, has become one of the most interesting aspect of individual, National and even international concern. The Objective/main benefit of this work is to keep criminals and unwanted guest away from our environments, Common sense dictates us to lock our doors at night and when we are away from home, but resi-dential crime prevention comes in many other shapes and sizes.

Effective residential crime prevention depends on everything from properly fitted doors to stopping your mail delivery when away on vacation.Not every intrusion can be prevented. Knowing what to do when faced with different situations not only protects your possessions but can save your life. Recently surveillance systems have become more important for everyone's security. The embedded surveillance system, frequently used in a home, an office or a factory, uses a sensor triggered to turn on a camera. Some designs use different types of sensors to achieve reliability by means of the different features of each sensor.

II. LITERATURE SURVEY

Keeping our home secure is one of responsible,but though at times even if we are responsible and taking care of our home,there are possible of intruders to make intrusion. Nowadays, Wireless Monitoring for home security is among the cutting-edge researches in the field of International Intelligent Building. To implement real-time surveillance of the home security, the intelligent remote monitoring system was developed for home security based on ZigBee technology and GSM / GPRS network. The system can send abnormal images and warning messages through MMS and SMS, receive remote instruction, and remote monitor household appliances. Meanwhile, the introduction of a variety of sensors and the enhancement of systempsilas reliability guaranteed that the intelligent remote monitoring system can be responsible for home security.The hardware and software design and system performance are expounded in details. The experimental result shows that the system can attain remote surveillance of intelligent home safety with high availability and reliability.[1].

Hardware and software design of multimedia sensor networks are proposed for smart home surveillance system, which employs multiple sensing and distributed processing and event-triggered surveillance. This network consists of the following two tiers: the wireless sensor network (WSN) tier is established on the IEEE 802.15.4/ZigBee protocol, constituting of scalar sensor nodes capable of capturing and processing scalar data and transmitting it to a sink node; the video surveillance network tier constitutes of multimedia sensor nodes connected by Ethernet, which can transmit multimedia content, such as compressed video and audio streams and the monitor data from the WSN tier, to the monitor center or user. Base on the designed multimedia sensor networks, the surveillance system can provide the user with harmful events alarms, event-triggered or continuous remote surveillance of his/her home.[2].

On the basis of temporal consideration we classify pixels into three classes: background, midground and foreground to distinguish between long-term, medium-term and short term changes. The algorithm has been implemented on a hardware platform with limited resources and it could be used in a wider system like a wireless sensor networks. Particular care has been put in realizing the algorithm so that the limited available resources are used in an efficient way. Experiments have been conducted on publicly available datasets and performance measures are reported.[3].

One important goal of surveillance systems is to collect information about the behavior and position of interested targets in the sensing environment. These systems can be applied to many applications, such as fire emergency, surveillance system, and smart home. Recently, surveillance systems combining wireless sensor networks with video cameras have become more and more popular. In traditional video surveillance systems, the system performance and cost is proportional to the number of deployed video camera. In this paper, we propose a real time video surveillance system consisting of many low cost sensors and a few wireless video cameras. The system allows a group of cooperating sensor devices to detect and track mobile objects and to report their positions to the sink node in the wireless sensor network. Then, the sink node uses the IP cameras deployed in the sensing area to record these events and display the present situations. We also propose a camera control scheme to initialize the coverage distribution of cameras and support the inter-task handoff operations between cameras. The result shows that our surveillance system is adaptable to variant environments and provides real time information of the monitored environment.[4].

As demand for surveillance of physical locations increases, automated decision making software can help maintain the rising costs of human monitoring. The variety in different types of sensors is also growing, and making use of their consolidated data can improve the decision making process. Using the constructive research method, we aim to define a design of a surveillance system's decision making component that utilizes data fusion from multiple types of sensors. As a solution we present the logical decision making server (LDMS), used in the single location surveillance point (SLSP), a system designed for monitoring an indoors location. The decision making capabilities in the LDMS are based on user-configurable security rules, which allow security personnel to define threats based on current and recent event reports from any or all of the environmentpsilas sensors. The LDMS has been successfully developed and integrated into an SLSP implementation.[5].

We design and implement a surveillance system based on an embedded system with multiple ultrasonic sensor modules to enhance the system's reliability. The ultrasonic sensor module includes a transmitter and a receiver, and they are placed in a line direction. Because the ultrasonic air transmission will spread a beam angle, we use multiple ultrasonic receivers to receive the ultrasonic transmission. If any intruder passes through the ultrasonic sensing area, the ultrasonic transmission will be blocked by a human body. As the receivers will not receive any ultrasonic transmission produced by the ultrasonic transmitter, the system will sense when someone has passed through the surveillance area. We use a Majority Voting Mechanism (MVM) for a group of sensors. If over half the sensors in a sensor group sense a signal blocking, then the majority voting circuit will send a trigger signal to the surveillance system.idle and is a potential candidate to turn off and save energy. Cold spot is tackled through migration.[6].

This deals with the design and implementation of Smart surveillance monitoring system using Raspberry pi and PIR sensor for mobile devices. It increases the usage of mobile technology to provide essential security to our homes and for other control applications . The proposed home security system captures information and transmits it via a 3G Dongle to a Smart phone using web application. Raspberry pi operates and controls motion detectors and video cameras for remote sensing and surveillance, streams live video and records it for future playback. It can also find the number of persons located with the help of the Infrared sensor.. For example , when motion is detected, The cameras automatically initiate recording and the Raspberry pi device alerts the owner of the possible intrusion having a smart phone. Raspberry- Pi has two main components interacting with each other: one is the Web Application that executes on the mobile device's browser and server-side scripts that run in a cloud which will be operated by the Raspberry Pi Hardware tool component.[7].

A low-power consumption remote home security alarm system developed by applying WSN and GSM technology is presented. It can detect the theft, leaking of raw gas and fire, and send alarm message remotely. The hardware of this system includes the single chip C5081F310, wireless receiving and sending chip CC1100 as well as the SIMENS TC35 GSM module and can send a piece of alarm short message to the user's mobile phone when some dangerous condition has been detected.[8].

III. PROPOSED WORK

Overall system architecture is shown in Fig.1,here with the fixed webcam at the door,where two sensors called Vibration sensor and PIR sensor is attached and that is connected to the Arduino Microcontroller where it controls and changes from analog to digital signals nad makes the camera to initiate and captures the image,where the password coder is fixed at the door,if the unknown person comes they will type the password and get inside the house an will get the notifications and images of the respective person,if it is intruder,if he tries to break the door,through the vibration sensor it senses and the image to the user,so that the user inform to the police to the nearby statio and police comes and catch the thief,here the cloud server is connected to the system for the back up and the android to it,from that to the user’s android notification will be arrived.There are seven modules that describes the each step of the project.

A.User Registration

This process is registered by providing Name, Mobile number, Address for communication & other personal information. User access the main server through ANDROID implementation to fetch out the image of the thief. Android SDK installed in a Android mobile platform of the user.

B.Reference Image Capturing

Web camera is connected with the place which is to be monitored. Once the admin locks the door, he will be switching on the Web camera device for capturing the image.kept as the Reference image for further computational process. This reference image is always compared with the next following images for the sake the intruder detection by applying Motion detection algorithm.

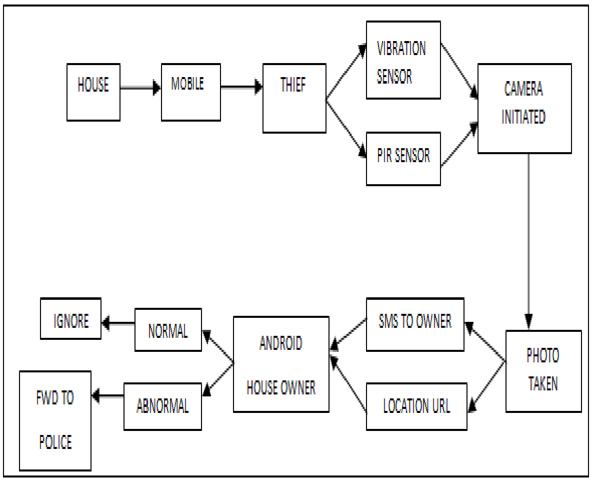


Fig. 1. System Architecture

C. Image Detection Process

Image detection process is applied to find out the Motion in a particular room. The web camera is kept for further process. The reference image which is taken by the camera is compared with the further images taken by the camera.If same image persist, the no alert is initiated, if some movement or the motion is detected by the web camera, immediately, the triggers .

D.Cloud Server.

The main server will have the database of the admin's mobile number and also the server is connected with the mobile phone for sending Alert SMS to the admin's mobile.

E.Vibration sensor and PIR sensor.

If Vibration sensor and PIR sensor detection is confirmed, immediately system initiates the Mobile phone connected with the server for sending Alert SMS to the Admin's Mobile number. Admin will be receiving an Alert SMS "Motion Detected" in their mobile phone. So PIR sensor is used to detect the human near to the door and Vibration sensor is used identify if any one rip the door

F.Arduino Microcontroller.

Arduino is an open-source electronics prototyping platform based on flexible, easy-to-use hardware and software.Vibration sensor and PIR sensor are connected with arduino board.It changes from analog to digital signals and sends to camera to initiate and generally through USB we can send details or images or any information to our android as shown in Fig.2.

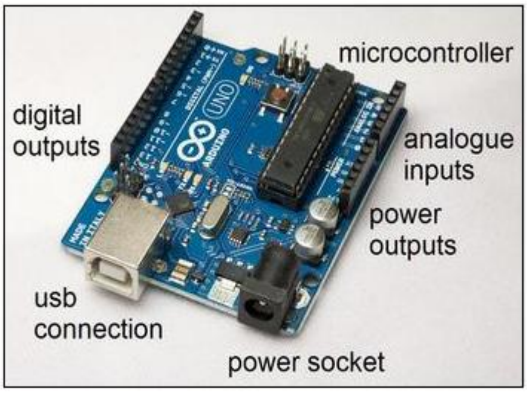


Fig. 2 . Ardunio Microcontroller

G.SMS alert to Owner

Once after receiving the alert SMS and location of the house to the adman's mobile, admin will then login through his mobile to access Main Server via ANDROID package which is installed in his mobile.Admin can see whether, the really thief has entered in or the Genuine people entry via Image which is recorded by the web camera then after initiating Alert SMS. The admin can decide then after either to neglect, if any genuine person has entered, or take action if thief has entered he can call to the police and the location is send to the police.

IV. RESULTS AND DISCUSSION

With the usage of the Arduino controller,the information the notification will be received bit fast than using normal microcontrollers where the user can take the action immediately and inform to the police where according to that we can make our home secure at the time if the intrusion takes place.

And it is discussed to make certain changes in future where without using of any sensors to keep our home secure.

The results can predict like number of intrusions can reduce due to the usage of sensors where instead of attaching CCTV or single webcam,by using so these sensors,we can easily come to know about the intrusion and can be even calm though intrusion takes place because we will somehow come to know about it and can inform to the police though we are not at home,

V. CONCLUSION AND FUTURE WORK

In the proposed work the secutity level is increased due to the usage of the arduino microcontroller which sends the images to the user, has in-built capabilities and is easily connectible to external devices. In future,instead of using multiple sensors and a linking between them,the functionality of both sensors can be incorporated into single device for generating trigger fastly to the users.

REFERENCES

[1] Jun Hou, Chengdong Wu, Zhongjia Yuan, Jiyuan Tan, Qiaoqiao Wang and Yun Zhou, "Research of Intelligent Home Security Surveillance System Based on ZigBee," International Symposium on Intelligent Information Technology Application Workshops, Shanghai, 21-22

Dec. 2008, pp. 554-57.

[2] Xiangjun Zhu, Shaodong Ying and Le Ling “Multimedia sensor networks design for smart home surveillance,” Control and Decision Conference, 2008, Chinese, 2-4 July 2008, pp. 431-435

[3] L. Lo Presti, M. La Cascia, “Real-Time Object Detection in Embedded Video Surveillance Systems,” Ninth International Workshop on Image Analysis for Multimedia Interactive Services, 7-9 May 2008, pp. 151-154.

[4] Wen-Tsuen Chen, Po-Yu Chen, Wei-Shun Lee and Chi-Fu Huang, “Design and Implementation of a Real Time Video Surveillance System with Wireless Sensor Networks,” VTC Spring 2008. IEEE Vehicular Technology Conference, 11-14 May 2008, pp. 218-222.

[5] Mikko Nieminen, Tomi Raty, and Mikko Lindholm, “Multi-Sensor Logical Decision Making in the Single Location Surveillance Point System,” Fourth International Conference on Systems, France, 1-6 March 2009, pp. 86-90

[6] Ying-Wen Bai, Li-Sih Shen and Zong-Han Li, “Design andImplementation of an Embedded Surveillance System by Use of Multiple Ultrasonic Sensors”, The 28th IEEE International Conference on Consumer Electronics, Las Vegas, Nevada, USA, 11-13 Jan. 2010, 11.1-3, pp. 501-502.

[7] Smart Surveillance Monitoring System Using Raspberry PI and PIR SensorSanjana Prasad et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 7107-7109

[8] A Remote Security System Based on WirelessSensor Networand GSM Technology Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second InternationalConference on (Volume:1) 25 April 2010

SURVEY ON BIOMEDICAL IMAGE RETRIEVAL TECHNIQUES

Sofia Mehraj. A[#1], Rajeswari. R[*2]

[#1]*Research Scholar, Department of Computer Application,Bharathiar University,Coimbatore.*
[*2]*Assistant Professor, Department of Computer Application,Bharathiar University,Coimbatore.*

Abstract- **Biomedical image retrieval is one of the important research areas in recent years. A lot of work has been carried out in this area. There are various steps involved in biomedical image retrieval. They preprocessing including filtering, feature extraction and clustering. This paper gives an overview of these stages of biomedical image retrieval. This paper also presents a detailed study about various biomedical image retrieval techniques available in the literature.**

Keywords - **Biomedical image retrieval, Preprocessing, Filtering, Indexing, Feature extraction.**

I. INTRODUCTION

The medical image retrieval approaches and systems began as a research field exceeding across several domains. There are many challenges associated with image retrieval systems such as the incapability of image processing algorithm to identify the content of image automatically to support information retrieval lack of vigorous test collections, and appropriate queries to compare the system performance [1]. The medical image retrieval in radiology department of hospitals is equipped with Picture Archiving and Communications Systems (PACS) [2]. The storage, retrieval and transfer of images with several modalities are stored in PACS or on web. The DICOM (Digital Imaging and Communications in Medicine) format is used to store a PACS image [2]. This paper gives an overview of various techniques proposed in the literature for content based medical image retrieval. The paper
also introduces the basics of content based image retrieval systems. The organization of the paper is as follows. In Section 2, an introduction about image retrieval system is given. In Section 3, literature survey of existing medical image retrieval systems is given. Finally in Section 4, conclusion is given.

II. IMAGE RETRIEVAL SYSTEM

An image retrieval system is a system for browsing, searching and retrieving images from a large database of images. The medical image categorization, classification, indexing, registration, feature extraction and retrieval are performed over the entire image database in the Image Retrieval Systems [3].

In Content Based Image Retrieval (CBIR) the color is most frequently used visual feature due to its invariance with scaling, translation and rotation to its component value color space of image [4]. Content-based image retrieval systems commonly define visual similarity as a distance between extracted visual descriptors. Unfortunately, computing this distance exactly can be an expensive operation that increases the response time of a retrieval system [5]. In contrast to traditional text-based approaches which perform retrieval only at a conceptual level, the recently developed content-based image retrieval (CBIR) methods support full retrieval by visual content or properties of images, i.e., retrieving image data at a perceptual level with the objective and quantitative measurements of the visual content and integration of image processing, pattern recognition and computer vision [4]. The Content based image retrieval system seeks out the image via automatically derived image features, such as color, texture and shape. The main drawback for CBIR technique is that, there is semantic gap between high level and low level features, next the problem involves entering an image as a query into a software application that is designed to employ CBIR techniques in extracting visual properties and matching them [6].

2.1 Image Filtering

Filters are mainly used to increase contrast and brightness of an image as well as removing of noise. Filters will change the appearance of an image or part of an image by altering the shades and colors of the pixels in some technique. The irrelevant images are filtered out by using filtering approach for reducing the search space for similarity matching [7].

The multi-resolution Gaussian filter converts the 2D image into 3D plane [13]. The biomedical image retrieval is applied in various scales of Gabor filter [8]. The Wiener filter is finer in balancing between smoothness and accuracy while combined with DTCWT (Dual Tree Complex Wavelet Transform) than with DWT [9]. The Median filtering is enormously used in smoothing and denoising of biomedical images [10]. The two dimensional wavelet filters perchance by using one dimensional wavelet and scaling function [11].

2.2 Image Indexing

In the image indexing the k-means clustering algorithm is used to index the data objects for each dimension to attain number of ranges in an image [12]. For describing image indexing the MPEG-7 features are used, the features which are the mixture of color and texture using medical application. The color features are color layout, scalable color and color structure; and the texture feature are the edge histogram [13]. There are three various comparisons made in image retrieval namely distance-based indexing, cluster based indexing and multidimensional scaling [12]. In multidimensional scaling method the Spatial Access Methods [14] (SAM) index are defined by the data feature vector. The tree data structure with data nodes are leaves and cluster as hierarchy [12].

2.3 Feature Extraction

Feature extraction plays a major role in extracting image into meaningful region. Therefore the system becomes efficient and faster and also it reduces the system storage space. If the feature extraction is applied on the entire image, then the content becomes global features. In order to gain more feature the image is sub-divided into small areas, and features are extracted from these small regions and this method of extracting features is known as local feature extraction [4]. The low level features are texture, color and shape. The texture feature like Gabor wavelet filter [40], GLCM features [15] are more effective. In color feature the RGB color with color histogram properties are used. The shape feature is used to identify the object in an image. These low level features are briefly described in this section.

2.3.1 Image Features:

Feature extraction is the basis of content-based image retrieval. Within the visual feature scope, the features can be further classified as general features and domain specific features [16].The former include color, texture and shape features while the latter is application-dependent and may include, for example, human faces and finger prints. General visual features such as Shape and Texture are most widely used in CBMIR [17].

2.3.2 Texture Features:

Texture refers to visual patterns with properties of Homogeneity and consists of basic prmtvsor microTxlspatterns)whose spatial distribution in the image creates the appearance of a texture [18]. The rotation-invariant polar-wavelet texture feature for image retrieval involves a polar transform followed by an adaptive row shift invariant wavelet packet transform [19]. The statistical texture features provides the information about the properties of the intensity level distribution in the image like uniformity, smoothness, flatness, contrast and brightness [20]. The Grey-Level Co-occurrence Matrix (GLCM) was proposed by Haralick [14]. GLCM contains texture information about the frequency of occurrence of two grey-level neighboring pixel combination in an image [21].The five features which are intended to describe texture: Contrast, Homogeneity, Dissimilarity, Energy and Entropy.

2.3.3 Shape Features:

In medical image retrieval the shape is an important feature. The contour based and the regions based are the two types of approaches in shape feature [22]. The two approaches are used to extract an object in an image. The shape feature is incorporated from one form to another by using content based image retrieval system [23]. An object shape feature gives a meaningful role to identify and recognize the object [23, 24]. It is efficient and robust in providing the information to detect and recognize the object [24]. Contour based methods use only the boundary information. Region based methods use information from both the boundaries and interior region.

2.3.4 Color Features:

In the image retrieval only the color feature is not much systematic and effective. When combined with shape feature the color feature becomes more robust in searching for images [25]. In an image the state of the primary color and pixel color order alteration used the mean value and the standard deviation. The global attribute of an image is the color distribution [26]. The frequently used color descriptors are color histogram, color correlograms, coherence vectors, color moment [27]. The color histogram shows the color distribution of pixel in an image. There are 224 different possible colors of a color pixel [28]. The color correlogram shows both the color distributions of pixels and the spatial correlation of pairs of colors [4].The color coherence vectors incorporating spatial information into the color histogram [29]. The color moment is very dense in representation of colors with the mean, variance and skewness for individual component of color [4]. The k-nearest neighbor search helps in retrieving an image from a database by using extracted color features [27].

III. LITERATURE SURVEY

Chi-Ren Shyu et al (1999) [30] introduced the human-in-the-loop approach or a physician-in the-loop approach. This approach demarcates the Pathology Bearing Region (PBR) for human and set of anatomical landmark. The approach smeared to low-level computer vision and image processing algorithms to extract attributes associated to the dissimilarities in gray scale, texture, shape, etc. The location of PBR is recorded with respect to anatomical landmarks by using relational information. Finally the multidimensional index based on attributes value assigned to each image.

Antani et al (2004) [31] introduced the technique for hybrid text and image query retrieval. Here the author formed x-rays images of cervical and lumbar spine counting more than 17,000 digitized images. Here also created large number of digitized 35mm color slides of uterine cervix in the second National Health and Nutrition Examination Survey (NHANES II). The author developed a challenging in Content Based Image Retrieval Images and produced results.

Petrakis et al (2002) [32] introduced ImageMap for indexing and searching image databases (IDBs). In this author describes the Attributed Relational Graphs (ARGs), it is the general image content. In realistic medical images the ImageMap is tested. It provided visualization of dataset, clustering and data mining. It also achieves nearly 1,000 fold speed-up in search in sequential scanning.

Lehmann et al (2004) [33] developed the Image Retrieval in Medical Applications (IRMA). It is targeted at all-purpose structure in case-based reasoning or evidence-based medicine for semantic content analysis which is suitable for numerous applications. There are six layers of information modeling namely; feature layer, raw data layer, scheme layer, registered data layer, knowledge layer and object layer. In this the distributed system is implemented using multilayer processing. The core element for implementation is program sources, processing schemes, images, features, and blob trees. Finally the graphical user interface provides data entry and retrieval for web server.

Niblack et al (1993) [34] developed a QBIC (Query By Image Content). It describes the technique to query on-line huge image databases using the query from the image content. The content of the images are texture, color and shape of the image objects and region. The attributes of images and objects which give useful information of query functionality are used by the retrieval methods. It also produces the result using some algorithm for features like texture, color, shape and sketch query.

Smith et al (1996) [36] introduced the VisualSEEK system. The author describes that in an image database the visual feature are searched by the highly functional prototype system. The user can form the queries by diagramming spatial arrangements of color regions. Regarding the queries, the system indexes and automatically extracts prominent color regions from the images. An extensive diversity of complex joint color and spatial queries has been computed by utilizing effective indexing techniques for color information, region sizes and absolute spatial locations.

Bach et al (1996) [37] have developed Virage image search engine; which provides an open framework for construction system. The Virage engine states the visual features as the image „rmtvs.Tefaueare texture, shape or color. It is mainly used for face recognition and cancer cell detection. The revolution from data-rich illustration of clear image pixels to a compact and semantic-rich illustration of visually prominent characteristics are the architecture of the system.

Cao et al (2011) [38] have introduced the Medical Multimedia Analysis and Retrieval (MMAR2011) system. This paper tells about the sensor technology, massive digital storage, processing speed and high speed networking are united into the medical application. Medical multimedia data are captured in huge amount and recorded in digital format in regular medical practice, education and research. Intellectual medical ideas are Table 1 gives a summary of the existing medical image retrieval systems described in this section.

Thies et al (2005) [39] have developed CasImage database with the IRMA framework. The IRMA (Image Retrieval in Medical Application) framework rigorously splits the data administration and the application logic. The CasImage dataset is used to evaluate the query performance of the ImageCLEF without optimizing the features in the IRMA corpus. Finally without the time consumption parameter adjustment and substantial loss of excellence retrieval, the parameter transformation is applied.

Table 1: Summary of existing medical image retrieval techniques discovery and retrieval from medical multimedia data in useful and extremely desirable manner.

Sl. No.	Biomedical Image Retrieval System	Database	Features used
1	ASSERT (Automatic Search and Selection Engine with Retrieval Tools)[30]	High-Resolution Computed Tomography (HRCT) of lungs image database	Texture, Shape, Edges,and Gray-scale Properties
2	NHANES II (The Second National Health And Nutrition Examination Survey) [31]	Cervical and lumbar spine X-ray images	Shape Features
3	ImageMap [32]	Multiple organs of Images	Individual Regions and Spatial Relationship
4	IRMA (Image Retrieval in Medical Applications) [33]	Various image modalities	Registration, feature extraction, selection, indexing, retrieval
5	QBIC (Query By Image Content) [34], [35]	Query on-line image databases	Color, text retrieval, high dimensional
6	Visual SEEK [36]	Various color image database	Image indexing, spatial query, global color histogram
7	VIRAGE [37]	Face recognition and cancer cell detection	Color, composition, layout, boundary information, texture.
8	MARS (Multimedia Analysis and Retrieval System) [38]	Medical multimedia data	Shape, color and texture
9	CasImage[39]	A variety of images from CT, MRI, and radiographs, to color photos	Global and Regional Color and Texture Features

IV. CONCLUSION

This paper summarizes the Image Retrieval used in medical application. A short description about the Content Based Image Retrieval (CBIR) in biomedical images is given. Then about the image filter and image indexing used for retrieving images in the CBIR. The paper also describes about the features such as texture, color and shape which are used in CBIR.

RGB IMAGE MULTI-THRESHOLDING USING OTSU AND CUCKOO SEARCH

S. Madhuvanthi#1, S. Bindhiya*2, J. Nisha*3

Department of EIE, St.Joseph's College of Engineering,

madhuvanthisridhar.163@gmail.com

Abstract— **Multi-level image thresholding is a well known image processing procedure. In this paper, RGB image segmentation is proposed using Cuckoo Search (CS) algorithm. The qualitative and quantitative investigation is carried out using the parameters, such as CPU time, between-class variance value and image quality measures, such as Mean Structural Similarity Index Matrix (MSSIM), and PSNR. Finally, this procedure is implemented to Extraction and Analysis of *T.cruzi* from the thin blood smear images. The study shows that, CS algorithm based multi-level segmentation offers good result on the considered RGB images.**

Keywords—multi-thresholding; RGB image;* T.cruzi, *Cuckoo search; PSNR; SSIM.

I. INTRODUCTION

Image thresholding is a preliminary image processing procedure, largely engaged to extract necessary information from gray scale and color images in various domains, such as medical, photography and geo science [4-6]. Multi-level thresholding is one of the image segmentation techniques, extensively considered to split an image into multiple regions or objects in order to discover and interpret any meaningful information within the image.

In the multi-level thresholding process, a threshold value (*T*) is chosen using a favorite signal processing scheme, which separates the image in to various clusters. For RGB images, finding the best possible threshold (*T*), which separates the image into foreground and background, remains a really significant step in image segmentation. Comprehensive evaluations on existing thresholding procedures can be found in the literature [1-12].

In this paper, Otsu's function based global thresholding scheme is considered for the multi-level segmentation of 512 x 512 sized RGB image dataset. The Otsu's between class variance method is combined with the Cuckoo Search (CS) algorithm, in order to increase the accuracy of the segmentation process. The segmentation accuracy is evaluated using familiar image quality measures, such as Mean Structural Similarity Index Matrix (MSSIM) and Peak Signal to Noise Ratio (PSNR) [5].Finally, the proposed on the *T.cruzi* thin blood smear image and the *T.cruzi* species is extracted from the image using the proposed segmentation technique.

II. OTSU

In this paper, image segmentation for the considered dataset is carried using Otsu's between-class variance method [7]. The optimal thresholds are attained by maximizing the objective function. A detailed description of Otsu's between-class variance method could be found in [4, 8-10].

In bi-level segmentation, the image is divided into two classes, such as C_0 and C_1 by a threshold at a level '*t*'. The class C_0 encloses the gray levels in the range 0 to t-1 and class C_1 encloses the gray levels from t to L – 1.

The probability allocation for C_0 and C_1 can be expressed as;

$$C_0 = \frac{p_0}{\omega_0(t)} \dots \frac{p_{t-1}}{\omega_0(t)} \quad \text{and} \quad C_1 = \frac{p_t}{\omega_1(t)} \dots \frac{p_{L-1}}{\omega 1(t)} \qquad (1)$$

where $\omega_0(t) = \sum_{i=0}^{t-1} p_i$ and $\omega_1(t) = \sum_{i=t}^{L-1} p_i$

The mean levels μ_0 and μ_1 for C_0 and C_1 can be written as;

$$\mu_0 = \sum_{i=0}^{t-1} \frac{ip_i}{\omega_0(t)} \quad \text{and} \quad \mu_1 = \sum_{i=t}^{L-1} \frac{ip_i}{\omega 1(t)} \qquad (2)$$

The mean intensity (μ_t)of the entire image can be represented as;

$\mu_T = \omega_0 \mu_0 + \omega_1 \mu_1$ and $\omega_0 + \omega_1 = 1$

The objective function for the bi-level thresholding problem can be expressed as;

$$\text{Maximize } J(t) = \sigma_0 + \sigma_1 \qquad (3)$$

For the multi-level thresholding process , let us take 'm' thresholds ($t_1, t_2, \dots, t_m$), which split the image into 'm' classes: C_0 with gray levels in the range 0 to t-1, C_1 with enclosed gray levels in the range t_1 to $t_{2\text{-}1}$, …, and C_m includes gray levels from tm to L – 1. The objective function for this problem can be expressed as;

$$\text{Maximize } J(t) = \sigma_0 + \sigma_1 + \dots + \sigma_m \qquad (4)$$

where $\sigma_0=\omega_0(\mu_0\text{-}\mu_t)^2$, $\sigma_1=\omega_1(\mu_1\text{-}\mu_t)^2$, … , $\sigma_m=\omega_m(\mu_m - \mu_t)^2$.

The well known parameters, such as the Root Mean Square Error (RMSE), the Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index Matrix (SSIM) are considered to evaluate the quality of the segmented image.

The mathematical expression is given below:

$$RMSE_{(x,y)} = \sqrt{MSE_{(x,y)}} = \sqrt{\frac{1}{MN} \sum_{i=1}^{H} \sum_{j=1}^{W} [x(i,j) - y(i,j)]^2} \qquad (5)$$

$$PSNR_{(x,y)} = 20 \log_{10} \left(\frac{255}{\sqrt{MSE_{(x,y)}}} \right); \text{dB} \qquad (6)$$

$$SSIM_{(x,y)} = \frac{(2\mu_x \mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 - C_1)(\sigma_{x^2} + \sigma_{y^2} + C_2)} \qquad (7)$$

Where *x* and *y* are original and segmented images; μ_x and μ_y are the average values, σ_{x2} and σ_{y2} are the variance, σ_{xy} is the covariance, and $C_1= (k_1L)^2$ and $C_2= (k_2L)^2$ stabilize the division with weak denominator, with L = 256, k_1 = 0.01, and k_2 = 0.03 [2]. In this work, RMSE, PSNR and SSIM are considered as the performance measure values.

III. OVERVIEW OF CUCKOO SEARCH ALGORITHM

Cuckoo Search (CS) algorithm was originally proposed in 2009, by mimicking the breeding tricks of parasitic cuckoos [14,15]. Due to its competence, CS was adopted by the researchers to solve the multi-level segmentation problems for gray scale images [1].

The mathematical expression of the CS considered in this study is given below:

$$x_i^{(t+1)} = x_i^{(t)} + \alpha \oplus Levy\ (\lambda) \qquad (8)$$

where $x_i^{(t)}$ is the initial position, $x_i^{(t+1)}$ is the updated position, α is chosen as 1.2 and $\oplus$ is the symbol for entry wise multiplication.

In this work, Levy Flight (LF) based search methodology is considered to update the position of the agents. Detailed description about LF can be accessible from [15]. It is a random walk in which the search steps can be drawn using the following Levy distribution

$$Levy \sim u = t^{-\lambda} \quad for \quad (1 < \lambda \le 3) \qquad (9)$$

In this work, the CS based optimization search is adopted to find the optimal thresholds for 512 x 512 sized RGB image dataset .

IV. RESULT AND DISCUSSIONS

This section presents the experimental results obtained for the RGB images and the *T.cruzi* blood smear image. In the proposed method, the following algorithm parameters are assigned during the heuristic search: Number of agents (*N*) = 15; dimension of search = *T*; iteration number (*t*) = 200; stopping criteria = J_{max}. In order to get the best possible threshold value, the experiment is repeated 30 times for every image with a preferred threshold (*T*) and the mean value among the trials is considered as the optimal value. The multi-thresholding procedure is implemented on RGB image dataset available at [16].

In this study, 512 x 512 sized RGB images, such as Aerial, Bridge, Cactus, and Geckos are chosen for the study. The image dataset and the corresponding histograms are presented in Table 1. In these histograms, the x-axis represents the RGB level and the y-axis denotes the pixel level.

Table 1. Image dataset and the corresponding RGB histograms

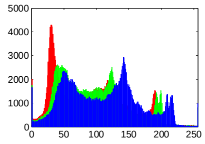
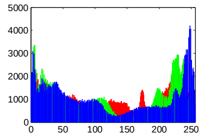
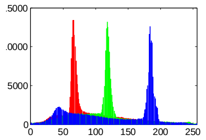
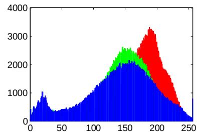
Test Image		RGB histogram
Aerial		
Bridge		
Cactus		
Geckos		

Table 2. Segmented Aerial image and optimal thresholds for T=2-5

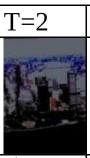
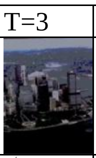
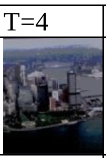
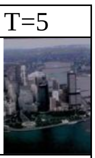
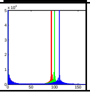
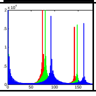
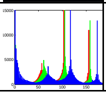
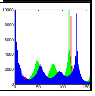
	T=2	T=3	T=4	T=5
Aerial				
				

Table 3. Comparison of MSSIM PSNR and CPU time

	T	MSSIM	PSNR	CPU time (min)
Aerial	2	0.3875	13.2264	0.3816
	3	0.5095	15.5972	0.5338
	4	0.6604	18.2926	0.6712
	5	0.7767	20.5815	0.7704
Bridge	2	0.4109	11.1224	0.3048
	3	0.6020	14.7739	0.5547
	4	0.6945	17.7418	0.6991
	5	0.7784	19.8840	0.7859
Cactus	2	0.5388	13.3915	0.4904
	3	0.6750	15.1963	0.6928
	4	0.8663	19.1970	0.8122
	5	0.8904	20.4207	0.8775
Geckos	2	0.5874	12.3545	0.6468
	3	0.7953	15.9112	0.8159
	4	0.8645	18.4774	0.8683
	5	0.8696	20.0463	0.8985

Multi-level segmentation is initially performed on the Aerial image using the CS algorithm for *T* = {2, 3, 4, 5} and the results are presented in Table 2 and Table 3.

From Table 3, it can be noted that, CS algorithm offers better performance measure values for *T* = {2, 3, 4, 5}. The computation time (CPU time in min) of the algorithm is computed using Matlab's time function. After getting the better result in the standard image dataset, the proposed method is considered to extract the *T.cruzi* species from the blood smear image available in DPDX image dataset.

T. cruzi causes the *Chagas Disease*, and it is a vector borne infectious disease due to kissing bug/ triatomine bug.

About the infection due to *T.cruzi:*

The recent report by World Health Organization (WHO) states that:

- Around 6 to 7 million people are expected to be infected by the Chagas Disease in Latin America**.**
- From Latin America, the desease has now spread to other continents.
- The disease can be curable if treatment is initiated soon after infection.
- In the chronic phase anti-parasitic treatment can also prevent or curb/halt disease progression.
- Up to 30% of chronically infected people develop cardiac alterations and up to 10% develop digestive, neurological or mixed alterations which may require specific treatment**.**

Hence, before suggesting any anti-parasitic drug to cure this infection, it is necessary to analyze the stage of the disease. Hence, blood screening is a vital procedure to analyze the stage. In this work, we considered a thin blood smear image and implemented the Otsu + CS based technique and the results are presented below:

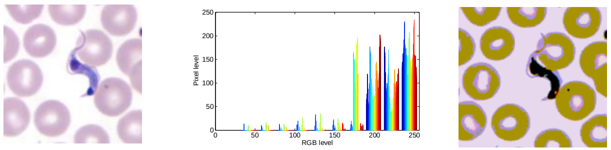
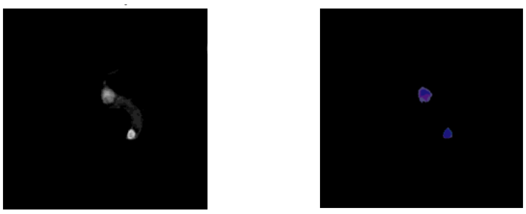


Image Histogram (c) Segmentation

Figure 1. Original blood smear image, RGB histogram and the segmented image for *T=2*



(a) Extracted - Gray (b) Extracted – Colour

Figure 2. Extracted T. cruzi

From Fig. 1 and 2 it can be observed that, this procedure is efficient in extracting the T. cruzi species from the RGB image. This procedure can also be used to detect the T. cruzi from thick blood smear images during the mass screening process. This image thresholding procedure can be used to assist the laboratory person who involved in the analysis of thin and thick blood smear images. This procedure can also be extended to analyze Maleria infections.

V. CONCLUSION

In this paper, a multi-level thresholding is presented for RGB image dataset using CS and Otsu's function. This work finds the optimal threshold for a chosen image with a chosen *T* value. The performance of the proposed method is analyzed using image quality measures, such as CPU time, SSIM, and PSNR. Finally it is validated using the thin blood smear image with T. cruzi. The OTSU and CS based approach offered better result in multi-level thresholding process.

REFERENCES

[1] Agrawal, S., Panda, R., Bhuyan, S., Panigrahi, B.K.: Tsallis entropy based optimal multilevel thresholding using cuckoo search algorithm, Swarm and Evolutionary Computation, **11**, 16–30 (2013)

[2] Akay, B.: A study on particle swarm optimization and artificial bee colony algorithms for multilevel thresholding, Applied Soft Computing, **13** (6), 3066–3091(2013)

[3] Larson, E. C., Chandler, D. M.: Most apparent distortion: Full-reference image quality assessment and the role of strategy, Journal of Electronic Imaging, **19** (1), Article ID 011006 (2010)

[4] Ghamisi, P., Couceiro, M. S., Martins, F. M. L., and Benediktsson, J. A.: Multilevel image segmentation based on fractional-order Darwinian particle swarm optimization, IEEE Transactions on Geoscience and Remote sensing, **52**(5), 2382-2394 (2014)

[5] Grgic, S., Grgic, M., Mrak. M.: Reliability of objective picture quality measures, Journal of Electrical Engineering, **55**(1-2), 3–10(2004)

[6] Manickavasagam, K., Sutha, S., Kamalanand, K.: Development of Systems for Classification of Different Plasmodium Species in Thin Blood Smear Microscopic Images, Journal of Advanced Microscopy Research, **9**, (2), 86-92(2014)

[7] Otsu, N.: A Threshold selection method from Gray-Level Histograms, IEEE T. on Systems, Man and Cybernetics, **9**(1), 62-66 (1979)

[8] Raja, N.S.M., Rajinikanth,V., Latha, K.: Otsu Based Optimal Multilevel Image Thresholding Using Firefly Algorithm, Modelling and Simulation in Engineering, vol. 2014, Article ID 794574, 17 pages (2014)

[9] Rajinikanth, V., Couceiro, M.S.: RGB Histogram Based Color Image Segmentation Using Firefly Algorithm, Procedia Computer Science, **46**, 1449–1457 (2015). Doi:10.1016/j.procs.2015.02.064.

[10] Rajinikanth, V., Sri Madhava Raja, N., Latha, K.: Optimal Multilevel Image Thresholding: An Analysis with PSO and BFO Algorithms, Aust. J. Basic & Appl. Sci., **8**(9), 443-454 (2014)

[11] Sezgin, M., Sankar, B.: Survey over Image Thresholding Techniques and Quantitative Performance Evaluation, Journal of Electronic Imaging, **13**(1), 146 – 165 (2004)

[12] Tuba, M.: Multilevel image thresholding by nature-inspired algorithms: A short review, Computer Science Journal of Moldova, **22**(3), 318-338 (2014)

[13] Wang, Z., Bovik, A.C., Sheikh, H. R., Simoncelli, E.P.: Image Quality Assessment: From Error VisibilitytoStructural Similarity, IEEE Transactions on Image Processing, **13**(4), 600 – 612 (2004)

[14] Yang, X.S., Deb, S.: Cuckoo search via Lévy flights. In: Proceedings of World Congress on Nature and Biologically Inspired Computing (NaBIC 2009), pp. 210–214. IEEE Publications, USA (2009)

[15] Yang, X.S: Nature-Inspired Metaheuristic Algorithms, Luniver Press, Frome, UK, 2008.

[16] http://vision.okstate.edu/?loc=csiq

MINING BIGDATA IN HEALTH CARE

B. Ilakiya1[#1,]K.Mownika[*2],R.Ezhilarasi[*3]

[#1]Student, III yr, Department of Computer science and Engineering, KarpagaVinayaga college of Engineering and Technology, Madurantagam.
ilakiyanavya@gmail.com[1]
mownikakavi@gmail.com[2]
ezhilarasi4010@gmail.com[3]

Abstract -**Mining the versatile large amount of data has been used intensively and broadly by several organizations. The applications can greatlybenefit all parties involved in the healthcare industry. The healthcare background is generally supposed asbeing information more yet knowledge less. There is a affluence of information obtainable within thehealthcare systems. However, there is a lack of useful analysis tools to realize hidden relationships andtrends in data. Knowledge discovery and data mining have established frequent applications in commerceand scientific domain. Valuable facts can be exposed from application of data mining techniques inhealthcare system. Likewise Immunization and vaccination have been used as an upstream, for protectingchildren, against such infections and infectious diseases as Polio, DPG, BCG and Measles. This critiqueexplores data mining applications in healthcare. In this study, we briefly examine the potential use ofclassification based data mining techniques such as decision tree, Artificial Neural Network to massivevolume of Immunization data.**

Keywords- Data Mining, Knowledge discovery, Artificial Neural Network

I. INTRODUCTION

Data Mining or "the efficient discovery ofvaluable, on-obvious information from a largecollection of datahas a goal to discoverknowledge out of data and present it in a form thatis easily comprehensible to humans. Knowledgedetection in databases is precise process consistingof a number of distinct stepsData mining is thefoundation step, which outcome in the discovery ofunknown but helpful knowledge from hugedatabases. A formal definition of Knowledgediscovery in databases is given as follows: “Datamining, or knowledge discovery, is the computerassistedprocess of digging through and analyzingenormous sets of data and then extracting themeaning of the data. Data mining tools predictbehaviors and future trends, allowing businesses tomake proactive, knowledge-driven decisions[3].Data mining expertise provide a consumerleaningapproach to new and unknown patterns inthe data.

The exposed knowledge can be used bythe healthcare administrators to progress thesuperiority of service.In healthcare, data mining is becominggradually more well-liked, if not ever moreessential. Several factors have motivated the useofdata mining applications in healthcare [4]. Theexistence of medical insurance fraud and abuse, forexample, has led many healthcare insurers toattempt to reduce their losses by using data mining tools to help them find and track offenders [5]Fraud detection using data mining applications isprevalent in the commercial world, for example, inthe detection of fraudulent credit cardtransaction[6].Recently, there have been reports of successfuldata mining applications in healthcare fraud andgreat asset to healthcare organizations, but theyhave to be first transformed into information. Thehealthcare industry can benefit greatly from datamining applications [13, 14]. The objective of thisarticle is to explore relevant data miningapplications by first examining data miningconcepts; then, classifying potential data miningtechniques in healthcare; and finally, highlighting the limitations of data mining and offering somefuture directions.

II. DATA MINING CONCEPTS

A. Definition

Data mining may be defined as “the explorationandanalysis, by automatic or semiautomatic means,of large quantities of data in order to discovermeaningful patterns and rules” . Hence, it maybe considered mining knowledge from largeamounts of data since it involves knowledgeextraction, as well as data/pattern analysis.

B. Tasks

Data mining techniques can be broadlyclassified based on what they can do, namelydescription and visualization; association andclustering; and classification and estimation, whichis predictive modeling. Description andvisualization can contribute greatly towardsunderstanding a data set, especially a large one, anddetecting hidden patterns in data, especiallycomplicated data containing complex and nonlinearInteractions.In association, the aim is to decide whichvariables go jointly [17]. For example, marketbasketanalysis (the most popular form ofassociation analysis) refers to method thatgenerates probabilistic statements such as, “Ifpatients undergo treatment A, there is a 0.35 probability that they will exhibit symptom Z” [18].With clustering, the objective is to group objects, such as patients, in such a way that objectsbelonging to the same cluster are similar andobjects belonging to different clusters aredissimilar.

Inclustering is usedto group readmitted patients to better profile andunderstand such patients.The most common and important applicationsin data mining probably involve predictivemodeling. Classification refers to the prediction of a target variable that is categorical in nature, suchas predicting healthcare racket. Estimation, onthe other hand, refers to the prediction of a targetvariable that is metric (i.e., interval or ratio) innature, such as predicting the length of stay or theamount of resource utilization. For predictivemodeling, the data mining techniques commonlyused include traditional statistics, such as multiplediscriminate analysis and logistic regressionanalysis. They also include non-traditional methodsdeveloped in the areas of artificial intelligence andmachine learning [21].The two for the most partsignificant models of these are neural networks anddecision trees. More details on data miningtechniques can be found in Berry and Linoff.

C. The Righteous Cycle of Data Mining

The four stages of the righteous cycle of data Mining are:
1. Categorize healthcare troubles issues: where the aim is to classify areas where patterns in data have the possible of providing value.

2. Techniques to renovate difficulty intoinformation: for this function, the created resultsneed to be tacit in order to make the righteous cyclesuccessful. Several pitfalls can obstruct with theability to use the results of data mining. Some ofthe pitfalls are bad data formats, confusing datafields, and lack of functionality. In addition,identifying the right source of data is crucial to theresults of the analysis, as well as bringing the rightdata together on the computing system used foranalysis.

3. Performing of the information: where the results from data mining are acted upon then fed into the measurement stage.

4. Evaluate the outcome: this measurementprovides the feedback for continuously improvingresults. These measurements make the righteouscycle of data mining righteous. Even though thevalue of measurement and continuous improvementis widely acknowledged, it is usually given lessattention than it deserves Fig 1: Data mining cycle

III. DATA MINING TECHNIQUES IN HEALTHCARE

There are different data mining techniquespresented with their appropriateness needy on thesphere application. Information presents a well builtbasic backdrop for quantification andassessment of domino effect. However, algorithmsbased on information need to be modified andscaled before they are practical to data mining.

A.Decision Tree:

Decision trees are a approach ofrepresenting a sequence of rules that lead to a set orvalue. As a result, they are used for directed datamining, mainly classification. One of the mainreward of decision trees is that the model is quite reasonable since it takes the form of explicit rules.This allows the evaluation of results and theidentification of key attributes in the process . It consisting of nodes and branches organized in theform of a tree such that, every interior non-leafnode is labeled with ideals of the attributes. The branches coming out from an inner node are labeledwith ideals of the attributes in that node. Each nodeis labeled with a rank (a worth of the goalcharacteristic). Treebased models which includeclassification and regression trees, are the commonimplementation of induction modeling. Decision tree algorithms such as CART, ID3, C4.5, SLIQ, SPRINT. The decision tree can be built from the very small training set (Table 1). In this tableeach row corresponds to a enduring record. We willrefer to a row as a data instance. The data setcontains three predictor attributes, namely Age,Gender, symptoms and one goal attribute, namelydisease whose values to be predicted fromsymptoms indicates whether the correspondingenduring have a certain disease or not.

FIGURE 1:----------------

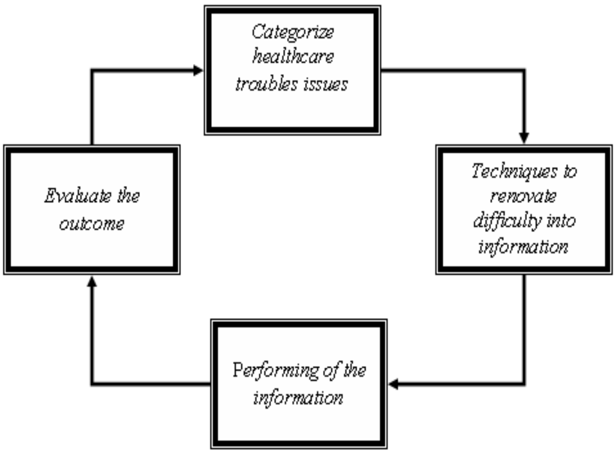
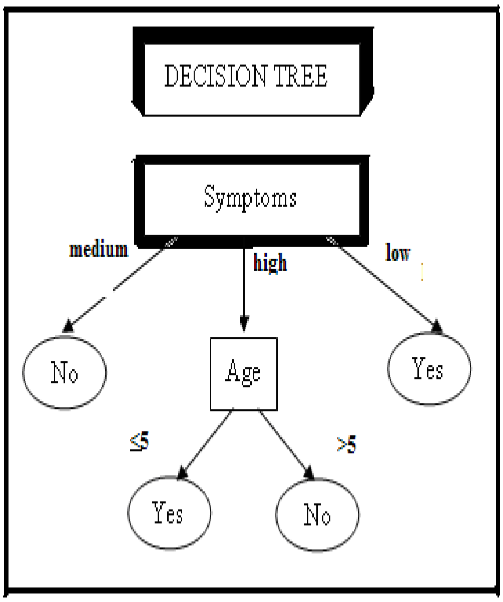

Categorize healthcare troubles issues
Techniques to renovate difficulty into information
Performing of the information
Evaluate the outcome

Table 1**:**

AGE	GENDER	SYMPTOMS	DISEASES
5	Female	Medium	Yes
3	male	High	Yes
4	Female	Medium	Yes
2	Female	Low	No
10	female	Low	No
9	Male	Low	No

Decision tree can be used to classify an poliodata of the above data set given in the Table 1. Theidea is to push the instance down the tree is shownin fig2, following the branches whose attributevalues match the instances attribute values, until theinstance reaches a leaf node, whose class label isthen assigned to the instance [25]. In this example,Gender attribute is irrelevant to a particularclassification task. The tree tests the intensity ofsymptom value in the instance. If the answer ismedium; the instance is pushed down through the corresponding branch and reaches the Age node. Then the tree tests the Age value in the instance. If the answer is 5, the instance is again pushed down through the corresponding branch. Now theinstance reaches the leaf node, where it is classifiedas yes.

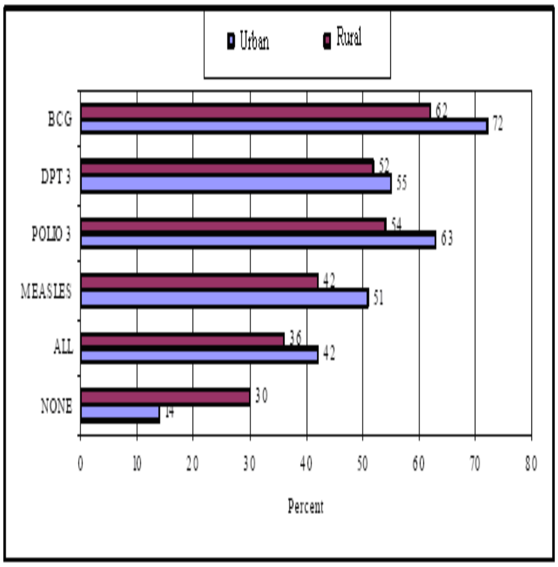
Fig. 2**: A DECISION TREE BUILD FROM A DATA:**



B.Artificial neural network (ANN):

A Neural network may be defined as "a modelof reasoningabuse detection [7]. Another factor is that the hugeamounts of data generated by healthcaretransactions are too complex and voluminous to be processed and analyzed by traditional methods.Data mining can improve decision-making bydiscovering patterns and trends in large amounts ofcomplex data.[8].Such analysis has becomeincreasingly essential as financial pressures haveheightened the need for healthcare organizations tomake decisions based on the analysis of clinical and64 financial data[9,10].

Insights gained from datamining can influence cost, revenue, and operatingefficiency while maintaining a high level ofcare.[11] Healthcare organizations that performdata mining are better positioned to meet their longtermneeds, Benko and Wilson argue.[12] Neural networks or artificial neural networksare also called connectionist system, paralleldistributed systems or adaptive systems becausethey are composed by a series of interconnectedprocessing elements that operate in parallel asshown in Fig. 3. A neural network can be definedas computational system consisting of a set ofhighly interconnected processing elements, calledneurons, which process information as a responseto external stimuli[28]. Stimuli are transmitted fromone processing element to another via synapses orinterconnection, which can be excitatory orinhibitory[29]. If the input to neuron is excitatory, itis more likely that this neuron connected to it.Neural networks are good for clustering,sequencing and predicting patterns but theirdrawback is that they do not explain how they havereached to a particular conclusion



Applications:

1. Image Analysis
2. Medical image processing [34]
3. Statistical Models for Breast
4. Cancer
5. [35]
6. Crohn's Disease and Ulcerative
7. Colitis
8. [36]
9. Classification of BloodCells [37]
10. Analysis of wave forms ECG [38]
11. Cervical cancer [39]
12. Tumors [40]
13. Retina damage classification [41]
14. Analysis of side drug effects [42]

IV. RESULTS AND DISSCUSSION

With the current rapid increase in the amountof medical data being collected electronically incritical care and the widespread availability ofcheap and reliable computing equipment, manyresearchers have already started, or are eager tostart, exploring these data. The outcome obtainedby data mining, in particular from the subfield ofmachine learning, may not only be oppressed torecover the worth of care by implement particularchange to care policies but can also be used as abasis for the structure of computer-based decisionsupportsystems.We present a case study of application of datamining and analyze data of children withImmunization details. The concept of Classificationmethod has been applied in the study of childvaccine. Polio is a opportune disease for datamining technology for a number of factors, thehuge amount of data polio virus invades the centralnervous system the spinal cord and the brain andmay cause weakness, paralysis, serious breathingproblems or death.

HealthCare administers wouldlike to know how to improve outcomes as much aspossible.Number of Reported Cases of Vaccine-Preventable Diseases.After preliminary results were analyzed, theprogram projected that over three million casesdeaths would be prevented and it has been resultedin a statistically significant . There is still, however, much that can bedone. Through the use of data mining algorithms itwas possible to verify the improvement of quality. Future work includes the Collecting informationabout levels of disease. In this study, noinformation about prevalence of disease wasavailable. It would be beneficial to compareimmunization uptake by district to disease levels inthose same areas, as immunization areas withhigher disease rates may be potential targets forfuture efforts and to obtain with higher accuracies in their prediction capabilities.

REFERENCES

[1] J.P. Bigus.(1996),"Data Mining with NeuralNetworks", New York: McGraw- Hill,.

[2] A survey of Knowledge Discovery and DataMining process[1] J.P. Bigus.(1996),"Data Mining with NeuralNetworks", New York: McGraw- Hill,.

[3] Data Mining in Healthcare: CurrentApplications and Issues By Ruben D. CanlasJr.Aug-2009.

A SURVEY ON ENERGY AWARE RESOURCE ALLOCATION TECHNIQUES IN CLOUD

Pavithra.B$^{\#1}$, Ranjana.R.^{*2}

$^{\#1}$*PG Student, Sri Sairam Engineering College, Chennai*

^{*2}*Associate Professor, Department of IT, Sri Sairam Engineering College, Chennai*

***Abstract* - Cloud Computing can be easily understood as internet based computing in which large groups of remote servers are networked to allow the centralized data storage and online access to computer services and resources. Cloud computing has emerged as the preeminent driver for distributed and shared computing. It is embraced by researchers, practitioners, and service providers across all industries around the world. Clouds have a prime focus to maximize the effectiveness of shared resources. Cloud resources are usually not only shared by multiple users but can be dynamically reallocated as per demand. The impact of cloud initiatives on how computing is performed is profound. Resource allocation is used to assign the available resources in an economic way. Resource Allocation Strategy (RAS) is all about integrating cloud provider activities for utilizing and allocating scarce resources within the limit of cloud environment so as to meet the needs of the cloud application. This paper gives an overview of comparison of the various existing scheduling techniques in cloud computing systems.**

***Keywords*- Cloud computing, Resource allocation, scheduling.**

I. INTRODUCTION

The Cloud Paradigm

Cloud Computing can be simply defined as computing in remote location or location independent with shared and dynamic resource availability on demand. Primary motive behind more organizations moving to cloud is the reduction in cost and dynamic resource allocation. It is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources. Cloud computing is an attractive computing model since it allows for the provision of resources on-demand. In a cloud computing environment, dynamic resource allocation and reallocation are keys for accommodating unpredictable demands and, ultimately, contribute to investment return.

Hence, the Cloud Computing is making our business application mobile and collaborative. The energy consumption and make span associated with the resources allocated should be taken into account. Resource allocation is the key technology of cloud computing, which utilizes the computing resources in the network to facilitate the execution of complicated tasks that require large-scale computation. Resource allocation needs to consider factors, such as load balancing, make span, and energy consumption.

A Resource Allocation System (RAS) in Cloud Computing can be seen as any mechanism that aims to guarantee that the applications requirements are attended to correctly by the provider's infrastructure. Cloud providers offer these computing resources as a service for their clients and charge them based on their usage in a pay-as-you-go fashion. Cloud clients submit requests to the cloud provider, specifying the amount of resources they need to perform certain tasks. Upon receiving a client request, the cloud provider scheduler creates a virtual machine (VM), allocates the requested resources to it, chooses one of the clusters to host the VM, and assigns the VM to one of the PMs within that cluster. The objective of this paper is to focus on various resource allocation techniques in cloud computing environment.

II. SIGNIFICANCE OF RESOURCE ALLOCATION

Resource allocation is a subject that has been addressed in many computing areas, such as operating systems, grid computing, and datacenter management. A Resource Allocation System (RAS) in Cloud Computing can be seen as any mechanism that aims to guarantee that the applications' requirements are attended to correctly by the provider's infrastructure. Along with this guarantee to the developer, resource allocation mechanisms should also consider the current status of each resource in the Cloud environment, in order to apply algorithms to better allocate physical and/or virtual resources to developers' applications, thus minimizing the operational cost of the cloud environment. The hardware and software resources are allocated to the cloud applications on-demand basis. For scalable computing, Virtual Machines are rented.

It requires the type and amount of resources needed by each application in order to complete a user job. The order and time of allocation of resources are also an input for an optimal RAS.From the cloud user's angle, the application requirement and Service Level Agreement (SLA) are major inputs to RAS.

III. ADVANTAGES OF RESOURCE ALLOCATION IN CLOUD

1) The biggest benefit of resource allocation is that user neither has to install software nor hardware to access the applications, to develop the application and to host the application over the internet.

The **aim** of resource allocation strategy is to maximize the profits of both the customer agent and the resource agent in a large datacenter by balancing the demand and supply in the market. Amount of energy consumed, cost incurred to provide services over the cloud, amount of execution time, these are major causes of concern and improvising the scheduling of tasks helps in minimizing these. Cloud Computing has many parameters and the scheduling to be applied depends upon user requirements. The aim of any scheduling algorithm is to meet used demand with minimum overheads.

1) Since users rent resources from remote servers for their purpose, they do not have control over their resources
2) Migration problem occurs, when the users wants to switch to some other provider for the better storage of their data. It's not easy to transfer huge data from one provider to the other.
3) In public cloud, the clients' data can be susceptible to hacking or phishing attacks. Since the servers on cloud are interconnected, it is easy for malware to spread.4) Peripheral devices like printers or scanners might not work with cloud. Many of them require software to be installed locally. Networked peripherals have lesser problems.5) More and deeper knowledge is required for allocating and managing resources in cloud, since all knowledge about the working of the cloud mainly depends upon the cloud service provider.

In cloud paradigm, an effective resource allocation strategy is required for achieving user satisfaction and maximizing the profit for cloud service providers. This paper proposes a comparative analysis of various existing resource scheduling algorithms in Cloud Computing environment, taking into consideration the for efficient management of data centers for cloud computing. Energy awareness and load balancing criteria for optimal performance of cloud data centers. These techniques focus on various parameters such as execution time, number of VMs, energy consumed, CPU Utilization, cost, available resources and number of requests.

Cloud Computing can be easily understood as internet based computing in which large groups of remote servers are networked to allow the centralized data storage and online access to computer services and resources. Cloud computing has emerged as the preeminent driver for distributed and shared computing. It is embraced by researchers, practitioners, and service providers across all industries around the world. Clouds have a prime focus to maximize the effectiveness of shared resources. Cloud resources are usually not only shared by multiple users but can be dynamically reallocated as per demand. The impact of cloud initiatives on how computing is performed is profound. Resource allocation is used to assign the available resources in an economic way. Resource Allocation Strategy (RAS) is all about integrating cloud provider activities for utilizing and allocating scarce resources within the limit of cloud environment so as to meet the needs of the cloud application. This paper gives an overview of comparison of the various existing scheduling techniques in cloud computing systems.

Resource allocation is a subject that has been addressed in many computing areas, such as operating systems, grid computing, and datacenter management. A Resource Allocation System (RAS) in Cloud Computing can be seen as any mechanism that aims to guarantee that the applications' requirements are attended to correctly by the provider's infrastructure. Along with this guarantee to the developer, resource allocation mechanisms should also consider the current status of each resource in the Cloud environment, in order to apply algorithms to better allocate physical and/or virtual resources to developers' applications, thus minimizing the operational cost of the cloud environment. The hardware and software resources are allocated to the cloud applications on-demand basis. For scalable computing, Virtual Machines are rented.

2) The next major benefit is that there is no limitation of place and medium. We can reach our applications and data anywhere in the world, on any system.
3) The user does not need to expend on hardware and software systems.
4) Cloud providers can share their resources over the internet during resource scarcity.

IV. LIMITATIONS OF RESOURCE ALLOCATION IN CLOUD: SOME OPEN ISSUES

1) Since users rent resources from remote servers for their purpose, they do not have control over their resources
2) Migration problem occurs, when the users wants to switch to some other provider for the better storage of their data. It's not easy to transfer huge data from one provider to the other.
3) In public cloud, the clients' data can be susceptible to hacking or phishing attacks. Since the servers on cloud are interconnected, it is easy for malware to spread.4) Peripheral devices like printers or scanners might not work with cloud. Many of them require software to be installed locally. Networked peripherals have lesser problems.5) More and deeper knowledge is required for allocating and managing resources in cloud, since all knowledge about the working of the cloud mainly depends upon the cloud service provider.

V. THE RESOURCE STRATEGY

The **aim** of resource allocation strategy is to maximize the profits of both the customer agent and the resource agent in a large datacenter by balancing the demand and supply in the market. Amount of energy consumed, cost incurred to provide services over the cloud, amount of execution time, these are major causes of concern and improvising the scheduling of tasks helps in minimizing these. Cloud Computing has many parameters and the scheduling to be applied depends upon user requirements. The aim of any scheduling algorithm is to meet used demand with minimum overheads.

VI. ANALYSIS OF EXISTING RESOURCE ALLOCATION TECHNIQUES IN CLOUD

S.No	Paper Title	Techniques Used	Metrics Considered	Advantage	Disadvantage
1	Energy efficient scheduling of virtual machines in cloud with deadline constraint. [1]	Energy efficient scheduling algorithm, EEVS is used and can support DVFS well.	Number of virtual machines and Performance – Power ratio.	Reduces the total energy consumed by the cloud. Higher optimal performance power ratio.	It does not suit for I/O-intensive or network-intensive VMs. The execution time and power consumption are ignored.The assumptions do not work well in practical cloud environment
2	Real-Time Tasks Oriented Energy-Aware Scheduling in Virtualized Clouds. [2]	Rolling-horizon scheduling called Energy-Aware Rolling-Horizon scheduling algorithm or EARH is used.	Task count and Task arrival rate, Task Deadlines.	Virtualization technique increases resource utilization and reduces energy consumption.	Difficult to implement in real cloud environment. The maximum amount of CPU cycles assigned to a VM that runs a task must be updated dynamically.
3	Optimized task scheduling and resource allocation on cloud computing environment using Improved Differential Evolution Algorithm (IDEA). [3]	IDEA Combines Taguchi method and DEA.	Cost versus Time.	High effectiveness and easy optimization.	The processing time of each subtask is resource dependent. Pre-emption is not allowed.

4	An Energy-Aware Fault Tolerant Scheduling Framework for Soft Error Resilient Cloud Computing Systems. [4]	The fault tolerant cloud scheduling framework is composed of two phases: Static scheduling and dynamic scheduling.	Slack, Application Index and Replication factor considered.	CSP to achieve high error coverage and fault tolerance confidence while minimizing global energy costs under user deadline constraints.	Does not guarantee to execute within deadlines. Cannot guarantee high compatibility among more than two VMs on the same machine.
5	More than bin packing: Dynamic resource allocation strategies in cloud data centers. [5]	Static and dynamic allocation. Bin packing heuristics	Time and Active Server Count.	Increases resource Utilization. Demand-based placement controllers in combination with a reallocation controller appear to be the most energy-efficient solution.	Reservation-based controllers have more migration and thereby high overload.
6	Efficient Multi-Tenant Virtual Machine Allocation in Cloud Data Centers. [6]	Uses Internet Data Centers (IDCs). LP-MKP Algorithm (Layered Progressive Multiple Knapsack Problem)	Maximum idle resources (Greedy), maximum available resources in the information tree and network diameters of similar tenant requests.	LP-MKP is significantly superior to the Greedy algorithm and better than the heuristic allocation algorithm MinTree and, it guarantees the fairness of resource allocation for similar tenant requests.	Obtaining the optimization goal is a tedious task. Integrating the LP-MKP algorithm into open-source cloud computing platforms, such as OpenStack and CloudStack needs to be considered.
7	Energy-Efficient Resource Allocation and Provisioning Framework for Cloud Data Centers. [7]	Data clustering (k-Means clustering), Workload prediction (Best Fit Decreasing) and Power management.	Sum of Squared Distances (SSD), Number of Clusters, and Execution time. Average CPU Utilization and Time.	This system is evaluated using real traces from Google cloud cluster. Achieves significant energy savings and high utilization that are very close to the optimal case.	Needs to test the framework on other cloud traces too. Must work to improve the workload prediction module in case of overhead evaluation of regular daily trends requests.
8	Resource Allocation Optimization in a Data Center with Energy Storage Devices. [8]	Convex optimization techniques	Relation between the cost function and the maximum charging/ discharging rate, ESD capacity	ESD management algorithm and the server consolidation have significant effects on reducing the total cost.	Analysis of the power hierarchy in a data center and the incorporation of more complex battery models needs to be addressed.
9	Dynamic Resource Allocation Using Virtual Machines for Cloud Computing Environment [9]	Skewness Algorithm, Server usage and resource allocation status. Hotspot Migration and Green Computing concept.	A set of overloaded resources in server and hot threshold for resource, along with temperature of a hot spot.	Achieves both overload avoidance and proper utilization of servers. Saves the energy using the green computing concept.	The evaluation of resource allocation status is based on the predicted future resource demands of VMs, hence prediction needs to be efficient to comply with real time requests.

10	A green energy-efficient scheduling algorithm using the DVFS technique for cloud datacenters. [10]	Green energy-efficient scheduling Algorithm, with extension of DVFS method and priority job scheduling	Number of Jobs versus Energy consumption and Execution time.	Satisfies the minimum resource requirement of a job and prevent the excess use of resources and increases resource utilization.	Servers chosen for a job have to satisfy the two proposed inequalities in this model. The system architecture is complicated to implement in real time cloud environment and heterogeneous servers.
11	Quality of Service Based Efficient Resource Allocation in Cloud Computing. [11]	Energy Aware Best Fit Decreasing (EABFD) algorithm.	Number of VM migrations, Percentage of SLA violations and Energy consumption versus Policy.	Energy consumption was reduced significantly and optimization of QoS is done by applying the EABFD with MAD RS Policy.	This model is implemented only in Cloud Sim toolkit. It needs to be extended for real time implementation.
12	Energy Aware Resource Allocation in Cloud Datacenter. [12]	VMs placement and VMs allocation policies using Modified Best Fit Decreasing (MBFD) and Migration algorithm. Uses Non Power Aware policy	Number of VMs and Energy consumed.	This proposed solution delivers both reliability and sustainability, contributing to our goals of optimizing energy utilization and reducing carbon emission.	There is more complexity of the migration algorithm that needs to be addressed while implementing.
13	Performance and Energy Efficiency Metrics for Communication Systems of Cloud Computing Data Centers.[13]	Proposes three metrics namely power-related metrics, performance-related metrics and network traffic-related metrics.	Communication Network Energy Efficiency(CNEE) and Network Power Usage Effectiveness (PUEE), Inter-Server Communication Latency (ISCL),	Analyzes end-to-end error rates at bit and packet levels to assure network performance and the desired level of QoS and helps detecting hardware faults.	The presented set of metrics needs to be standardized for performing evaluation in operational data centers.
14	Towards Energy-Efficient Cloud Computing: Prediction, Consolidation, and Over commitment. [14]	Workload prediction, VM placement and Workload Consolidation, and Resource Over commitment.	Time versus number of Requests and Saved Energy.	Resource over commitment has great potential for reducing cloud center energy consumption and solves under-utilization issues.	This requires the development of sophisticated resource management techniques that enables to reduce energy. One major problem with over commitment is PM overload, which needs to be addressed.
15	Energy-aware Load Balancing and Application Scaling for the Cloud Ecosystem. [15]	Energy-aware Scaling Algorithm with Load Balancing and energy-optimal operation regime	High-cost versus low-cost application scaling. Number of servers versus regime of operation.	Idle and lightly-loaded servers are switched to one of the sleep states to save energy. Attempts to maximize the number of servers operating in this regime.	Needs to evaluate the overhead. This needs to balance computational efficiency and SLA violations.

VII. CONCLUSION

Thus, cloud computing is a service that offers reliable IT infrastructure and software services off the user premises thereby saving cost on hardware, software, power and labour. An evaluation shows that dynamic resource allocation is the recent growing need of cloud providers satisfying more number of users and with the less response time. Cloud computing enables organization to reduce total cost of ownership on IT infrastructure on computing resource services, soft applications of distributed systems and data storage. In cloud paradigm, an effective resource allocation strategy is required for achieving user satisfaction and maximizing the profit for cloud service providers. This paper proposes a comparative analysis of various existing resource scheduling algorithms in Cloud Computing environment, taking into consideration the for efficient management of data centers for cloud computing. Energy awareness and load balancing criteria for optimal performance of cloud data centers. These techniques focus on various parameters such as execution time, number of VMs, energy consumed, CPU Utilization, cost, available resources and number of requests.

REFERENCES

[1] Youwei Ding, Xiaolin Qin , Liang Liu, Taochun Wang,“More than bin packing: Dynamic resource allocation strategies in cloud data centers '', Science Direct 2015.

[2] Jinn-Tsong Tsai Jia-Cen Fang , Jyh-Horng Chou, “Optimized task scheduling and resource allocation on cloud computing environment using Improved Differential Evolution Algorithm (IDEA) '', Science Direct 2014.

[3] Xiaomin Zhu, Laurence T. Yang, Huangke Chen Ji Wang, Shu Yin and Xiao cheng Liu, “Real-Time Tasks Oriented Energy-Aware Scheduling in Virtualized Clouds'', IEEE 2014.

[4] Youwei Ding, Xiaolin Qin , Liang Liu, Taochun Wang, “Energy efficient scheduling of virtual machines in cloud with deadline constraint'' , Science Direct 2015.

[5] Yue Gao Ming Hsieh, Gupta, S.K., Yanzhi Wang, “An Energy-Aware Fault Tolerant Scheduling Framework for Soft Error Resilient Cloud Computing Systems'', IEEE 2014.

[6] A.Wolke, M. Bichler, T., Setzer , “Planning vs. dynamic control-resource allocation in corporate clouds'', IEEE 2015.

[7] Y. Choi, S. Lee, J. Kim, Y. Kim, H. Pak, G. Moon, J. Ra, Y.-G. Jung ,“The method to secure scalability and high density in cloud data-center'', IEEE 2015.

[8] A. Beloglazov, J. Abawajy, R. Buyya, “Energy-aware resource allocation heuristics efficient management of data centers for Cloud computing'', Future Gener. Comput. Syst.2013.

[9] Atsuo Inomata, TaikiMorikawa, Minoru Ikebe, Sk.Md. Mizanur Rahman, “Proposal and Evaluation of Dynamic Resource Allocation Method Based on the Load Of VMs on IaaS'', IEEE 2014.

[10] Hadi Goudarzi and Massoud Pedram, “Maximizing Profit in Cloud Computing System Via Resource Allocation'', IEEE 2013.

[11] Riddhi Patel, Hitul Patel, Sanjay Patel, “Quality of Service Based Efficient Resource Allocation in Cloud Computing'', IJTRE 2015.

[12] Manasa H.B, Anirban Basu, “ Energy Aware Resource Allocation in Cloud Datacenter'', IJEAT 2013.

[13] Claudio Fiandrino, Dzmitry Kliazovich, Pascal Bouvry Albert Y. Zomaya, “Performance and Energy Efficiency Metrics for Communication Systems of Cloud Computing Data Centers'',IEEE 2015.

[14] Mehiar Dabbagh, Bechir Hamdaoui, Mohsen Guizani, Ammar Rayes, “Towards Energy-Efficient Cloud Computing: Prediction, Consolidation, and Over commitment'',IEEE 2015.

[15] Ashkan Paya and Dan C. Marinescu, “Energy-aware Load Balancing and Application Scaling for the Cloud Ecosystem'',IEEE 2015.

EVOLUTIONARY COMPUTATION TO DETECT DATA DUPLICATION USING GENETIC PROGRAMMING

L.Dharani#1
Dr.Vemuri Lakshminarayana*,D.Praveena Anjelin**
#1Assistant Professor, Department of Computer Science and engineering, Sree Sastha College of Engineering, Chennai , India
*Principal, Sree Sastha College of Engineering, Chennai, India
dharanimurugan10@gmail.com
**HOD/CSE, Sree Sastha College of Engineering, Chennai, India

Abstract- **The increasing volume of information available in digital media has become a challenging problem for data administrators. Usually built on data gathered from different sources, data repositories such as those used by digital libraries and e-commerce brokers may present records with disparate structure. Also, problems regarding low-response time, availability, security, and quality assurance become more difficult to handle as the amount of data gets larger. Databases may have “dirty” data (Replicas, Quasi Replicas, and Duplicates), because of dirty data we may get Performance degradation, Quality loss, Increasing operational costs. For replica-free repositories database has to be deduplicated (Duplicate detection / Data Cleaning). Deduplication is ideal for organizations wishing to backup, consolidate and improve performance during backups. In this paper, we propose a genetic programming approach to record deduplication that combines several different pieces of evidence extracted from the data content to find a deduplication function that is able to identify whether two entries in a repository are replicas or not and reduces overhead in human effort required to label training data.**

Keywords- **Machine Learning, Database administration, Deduplication, Data cleaning,**

I. INTRODUCTION

Increasing volume of information available in digital media has become a challenging problem for data administrators. Usually built on data gathered from different sources, data repositories such as those used by digital libraries and e-commerce brokers may present records with disparate structure. Also, problems regarding low-response time, availability, security, and quality assurance become more difficult to handle as the amount of data gets larger. Analyze the major consequences of allowing the existence of “dirty” data in the repositories. performance degradation as additional useless data demand more processing, more time is required to answer simple user queries, quality loss is the presence of replicas and other inconsistencies leads to distortions in reports and misleading conclusions based on the existing data, Increasing operational costs because of the additional volume of useless data, investments are required on more storage media and extra computational processing power to keep the response time levels acceptable.

1) Performance degradation—as additional useless data demand more processing, more time Is required to answer simple user queries;

2) Quality loss—the presence of replicas and other inconsistencies leads to distortions in reports and misleading conclusions based on the existing data;

3) Increasing operational costs—because of the additional volume of useless data, investments are required on more storage media and extra computational processing power to keep the response time levels acceptable.

The problem of detecting and removing duplicate entries in a repository is generally known as record deduplication.Record deduplication [1] is the task of identifying, in a data repository, records that refer to the same real world entity or object in spite of misspelling words, typos, different writing styles or even different schema representations or data types. Thus, there have been large investments from private and government organizations for developing methods for removing replicas from data repositories. In this project, we present a genetic programming (GP) approach to record deduplication. Our approach combines several different pieces of evidence extracted from the data content to produce a deduplication function that is able to identify whether two or more entries in a repository are replicas or not.

Our aim is to foster a method that finds a proper combination of the best pieces of evidence, thus yielding a deduplication function that maximizes performance using a small representative portion of the corresponding data for training purposes.[4] Then, this function can be used on the remaining data or even applied to other repositories with similar characteristics.

Advantage:

1.To reduce the additional useless data.

2.To reduce the processing time.

3.To reduce the extra computational processing power.

1.1 Genetic Programming:

In the field of artificial intelligence, genetic programming (GP) is a search heuristic that mimics the process of natural evolution. This heuristic is routinely used to generate useful solutions to optimization and search problems. Genetic algorithms belong to the larger class of evolutionary algorithms (EA), which generate solutions to optimization problems using techniques inspired by natural evolution, such as inheritance, mutation, selection,[6] and crossover.Genetic Programming, one of a number of evolutionary algorithms, follows Darwin's theory of evolution—often paraphrased as "survival of the fittest". There is a population of computer programs (individuals) that reproduce with each other. Over time, the best individuals will survive and eventually evolve to do well in the given environment.

II. METHODOLOGY

In Genetic Programming-The fundamental elements of an individual are its genes, which come together to form code. An individual's program is a tree-like structure and as such there are two types of genes: [8] functions and terminals. Terminals, in tree terminology, are leaves (nodes4 without branches) while functions are nodes with children. The function's children provide the arguments for the function. Creating a Random Population can be done by three techniques, namely grow, full and ramped-half and-half.Genetic programming find application in bioinformatics, phylogenetics, computational science, engineering, economics, chemistry, manufacturing, mathematics, physics and other fields. A typical genetic algorithm requires:

- A genetic representation of the solution domain
- A fitness function to evaluate the solution domain.

1.2.1 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. Certain selection methods rate the fitness of each solution and preferentially select the best solutions. Other methods rate only a random sample of the population, as the former process may be very time-consuming.

1.2.2 Genetic Operators

Two different genetic operators available. They are,

- Crossover (genetic algorithm)
- Mutation (genetic algorithm)

The next step is to generate a second generation population of solutions from those selected through genetic operators: crossover (also called recombination), and/or mutation. For each new solution to be produced, a pair of "parent" solutions is selected for breeding from the pool selected previously.[2] By producing a "child" solution using the above methods of crossover and mutation, a new solution is created which typically shares many of the characteristics of its "parents". New parents are selected for each new child, and the process continues until a new population of solutions of appropriate size is generated. Although reproduction methods that are based on the use of two parents are more "biology inspired", some research suggests that more than two "parents" generate higher quality chromosomes.

These processes ultimately result in the next generation population of chromosomes that is different from the initial generation. Generally the average fitness will have increased by this procedure for the population, since only the best organisms from the first generation are selected for breeding, along with a small proportion of less fit solutions, for reasons already mentioned above

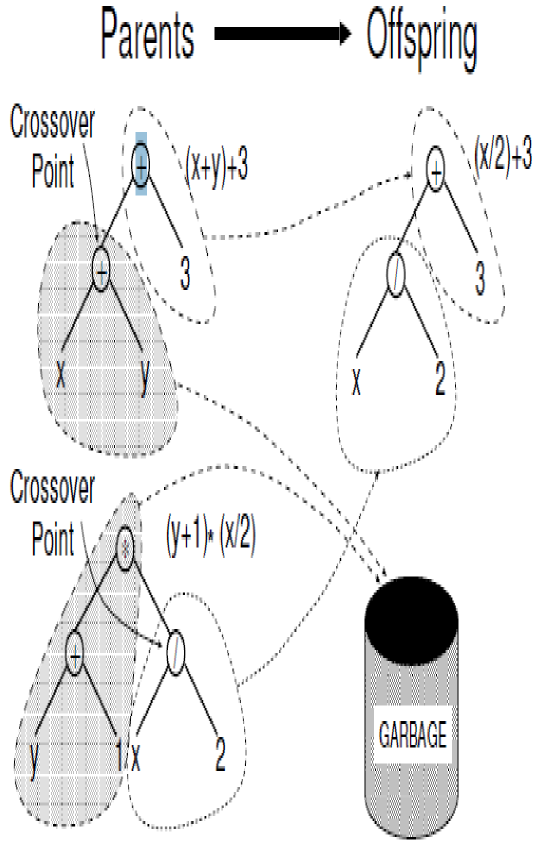


Fig:1.1 Example Subtree Crossover

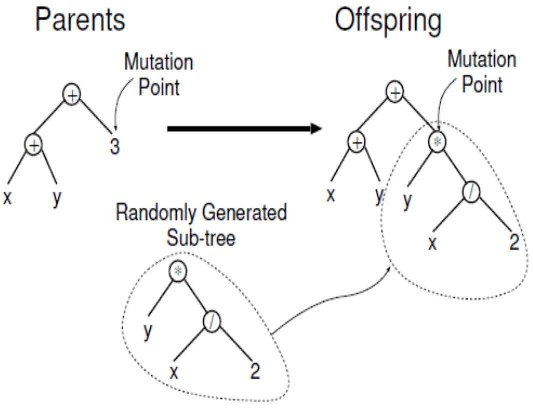


Fig:1.2 Example of Subtree Mutation

III. ALGORITHM

Genetic Programming:

1. Initialize the population (with random or user provided individuals).
2. Evaluate all individuals in the present population, assigning a numeric rating or fitness value to each one.
3. If the termination criterion is fulfilled, then execute the last step. Otherwise continue.
4. Reproduce the best individuals into the next generation population.
5. Select individuals that will compose the next generation with the best parents.
6. Apply the genetic operations to all individuals selected. Their offspring will compose the next population. Replace the existing generation by the generated population and go back to Step 2.
7. Present the best individual(s) in the population as the output of the evolutionary process.

IV. COMPARISON ANALYSIS

Usually, methods for data deduplication work in three distinct phases [11]: (1) generation of pairs of candidate records for comparison, which can, in the worst case, mean all possible pairs in the database, [2] calculation of some type of similarity between each pair based on their attributes, [3] classification of the pairs as replicas or not, depending on the similarity value found or a model learnt from data. In other deduplication methods,the process of labeling data can be extremely expensive or even unpractical. Furthermore, in some cases it is hard even for humans to decide if two records are replicas or not in the absence of enough information.

In this paper, GP is used to explore the vast space of existing similarity functions between records fields (or attributes), which can be created using many different combinations of weighted single-attribute similarity functions. At the same time that the method is capable of identifying the most relevant evidence, maximizing performance and potentially diminishing processing time, it also takes advantage of active learning to reduce the user effort in labeling data records.Methods such as decision trees, which incrementally select one attribute at a time to compose a decision model, GPs consider attribute interaction.

V. EXPECTED RESULTS

Deduplication is a time consuming task even for small collections, the implementation aim is to foster a method to find the weights, identification bounds and the best evidence that should be used for a given digital library.Deduplication by genetic programming-a machine learning approach provides solutions by specific genetic approaches like crossover and mutation are only the barest bones of real−world genetic systems. In most GP applications the candidate solutions in the population are assigned fitnesses independent of one another and interact only by competing for selection slots via their fitnesses.

Hence by providing proper replication boundary and fitness measure data duplication can achieve data reduction levels ranging from 10 to 1 to 50 to 1. With less storage needed, storage costs are reduced, because this means fewer disks and less frequent disk purchases. Less data also means smaller backups, which translates into smaller backup windows and faster recovery time objectives (RTO). The smaller backups also allow for longer retention times on virtual tape libraries (VTL) or archives.

VI. CONCLUSIONS

Identifying and handling replicas is important to guarantee the quality of the information made available by data intensive systems such as digital libraries and e-commerce brokers. These systems rely on consistent data to offer high-quality services, and may be affected by the existence of duplicates, quasi replicas, or near-duplicate entries in their repositories. Thus, for this reason, there have been significant investments from private and government organizations for developing methods for removing replicas from large data repositories. In this project, we presented a GP-based approach to record deduplication. Our approach is able to automatically suggest duplication functions

REFERENCES

[1].Alberto H.F. Laender, Alberto H.F. Laender , Marcos Andre´ Gonc¸alves,Moise´s G. de Carvalho, , MARCH 2012, “A Genetic Programming Approach to Record Deduplication” ieee transactions on knowledge and engineering, vol.24

[2].A.X. Falcao, W. Fan, and E.A. Fox, M.A. Gonc¸alves, J.P. Papa, R.d.S. Torres, B. Zhang ,2009, “A Genetic Programming Framework for Content-Based Image Retrieval,” Pattern Recognition, vol. 42, no. 2, pp. 283-292.

[3].M.G. de Carvalho, A.S. da Silva, M.A. Gonc¸alves, A.H.F. Laender, and 2006 “Learning to Deduplicate,” Proc. Sixth ACM/IEEE CS Joint Conf. Digital Libraries, pp. 41-50.

[4].Altigran S. da Silva, Gisele L. Pappa, Junio de Freitas, June2005, Active Learning Genetic Programming for Record Deduplication, ieee transactions on knowledge and engineering.

[5].N. Koudas, S. Srawagi, and D. Srivastava, 2006, “Record Linkage: Similarity Measures and Algorithms,” Proc. ACM SIGMOD Int’l Conf. Management of Data, pp. 802-803.

[6].I. Bhattacharya and L. Getoor, 2004 “Iterative Record Linkage for Cleaning and Integration,” Proc. Ninth ACM SIGMOD Workshop Research Issues in Data Mining and Knowledge Discovery, pp. 11-18,.

[7].S. Chaudhuri, K. Ganjam, V. Ganti, and R. Motwani, 2003, “Robust and Efficient Fuzzy Match for Online Data Cleaning,” Proc. ACM SIGMOD Int’l Conf. Management of Data, pp. 313-324.

[8].W. Banzhaf, F.D. Francone, P. Nordin, R.E. Keller, 1998, Genetic Programming - An Introduction: On the Automatic Evolution of Computer Programs and Its Applications. Morgan Kaufmann Publishers.

[9].B. Zhang, Y. Chen, W. Fan, E.A. Fox, M. Gonc¸alves, M. Cristo, and P. Calado, 2005, “Intelligent gp Fusion from Multiple Sources for Text Classification,” Proc. 14th ACM Int’l Conf. Information and Knowledge Management, pp. 477-484.

[10].M.G. de Carvalho, A.H.F. Laender, M.A. Gonc¸alves, and A.S. da Silva, 2008, “Replica Identification Using Genetic Programming,” Proc. 23rd Ann. ACM Symp. Applied Computing (SAC), pp. 1801-1806.

[11].M. Bilenko, R. Mooney, W. Cohen, P. Ravikumar, and S. Fienberg, Sept./Oct. 2003,“Adaptive Name Matching in Information Integration,” IEEE Intelligent Systems, vol. 18, no. 5, pp. 16-23.

ARCHITECTURAL APPROACH OF SECURITY IMPLEMENTATION IN MOBILE CLOUD COMPUTING

S.Premalatha, M.Preetha, S.Bhuvaneswari

Department of cse, panimalar engg college

premaselvan1995@gmail.com
m.preetha01@gmail.com
bhuvi.s2595@gmail.com

***Abstract*--During the last few years, there is a revolutionary development in the field of mobile computing, multimedia communication and wireless technology. Together with an explosive growth of the mobile computing and excellent promising technology of cloud computing concept, Mobile Cloud Computing (MCC) has been introduced to be a potential technology for mobile services. It is the trend in which resources are provided to a local client on an on-demand basis , usually by means of the internet. It is envisioned as a promising approach to augment computation capabilities of mobile devices for emerging resource-hungry mobile applications Although MCC provides many advantages, it reduces performance ,compatibility and lack of resources due to risk in security and privacy. Before mobile users could use a certain application, it should go through some level of threat evaluation. All file activities to be sent to mobile devices will be verified if it is malicious or not with the help of architectural approach. This paper will give a brief idea of implementing architectural approach for security in Mobile Cloud Computing .**

***Keywords*- MCC, Local client, Internet, Computation, Security ,privacy**

I. INTRODUCTION

Mobile devices, of all shapes and forms, are the fastest growing computing segment. While mobile devices are ubiquitous, they offer limited computation, storage and power. Cloud computing promises to fill this gap by providing computation and storage to mobile devices connected to the network. Cloud Computing is a model for enabling convenient, on demand network access to a shared pool of configurable resources (e.g. networks, servers, storage, applications and services) that can rapidly be provisioned and released with minimal management effort or service provider interaction. The rapid progress of mobile computing (MC)**[1]** becomes a powerful trend in the development of IT technology as well as commerce and industry fields. However, the mobile devices are facing many challenges in their resources (e.g., battery life, storage, and bandwidth) and communications (e.g., mobility and security)[2] .The limited resources significantly impede the improvement of service qualities. Mobile Cloud computing has been widely recognized as the next generation's computing infrastructure in mobile devices. MCC offers some advantages by allowing users to use infrastructure (e.g. server, networks, and storages), platforms (e.g., middleware services and operating systems), and software (e.g., application programs). Mobile cloud computing (MCC) is introduced as an integration of cloud computing into the mobile environment. Mobile cloud computing brings new types of services and facilities for mobile users to take full advantages of cloud computing .The various advantages [3] of MCC will extend battery lifetime, Improving reliability, scalability ,Multi-tenancy, data storage and processing.

The owner's data or files are saved in cloud server .Once the data is stored on the cloud ,Mobile cloud users does not have the data on their own device .so there may be a chance of unauthorized access to the data will harm the integrity of data .this introduces a risk in terms of data security and confidentiality. **so** security must be enhanced to ensure data integrity and confidentiality.

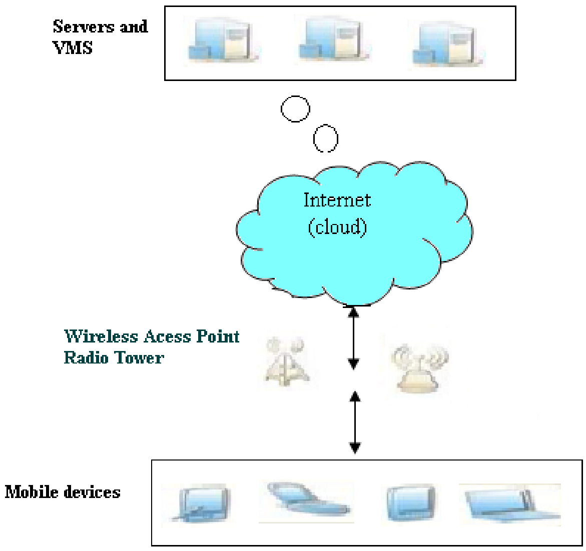


FIGURE 1 . Layout of MCC

II. RELATED WORK

The authors in [4] have discussed more information about the security problem in cloud. The authors analyze the security problem issues from cloud infrastructure point of view, the cloud user's point of view and at the end from cloud service deployment models point of view. From architecture prospective the cloud services providers want to implement multi-tenancy and elasticity as both these characteristics play a vital role in cloud security. From the cloud user's view, the security configuration needs to be implement so, each service should be sustained a level and at runtime. From service delivery model view, the Iaas, Paas and Saas models have security issues. The security issues of cloud management and cloud access method are also highlighted. The authors of [5] have proposed an overview of MCC security architecture. Data integrity and Privacy are important considerations of MCC security .Based on the security the author classifies the user into two categories: mobile network security and cloud security of mobile applications. The first category privacy and security of mobile applications are explained .

The second category is about securing the data on the cloud .The author portrays very dedicated issues associated with data integrity and data rights and authentication. The author in [6] have discussed about the security issues in which cloud service providers are facing .Therefore in order to ensure application and data security ,the cloud service providers must obey the manages Service Model(MSP) in the cloud environment. A detailed survey results which is conducted by International Data corporate(IDL) highlights that security is the major concern of IT executives in cloud service. There are many important issues and challenges which cloud computing is facing in the area of cyber security. In order to reduce the security issues, the cloud service providers must have to follow the standards like Information Technology Infrastructure Library (ITIL) and open Virtualization Format[OVF].The paper[7] discussed a detailed analysis of data security and privacy protection issues along with the existing solution to implement protection against these issues .The security architecture clearly shows the infrastructure, platform, software, security along with the services related to auditing and compliance. In [8] the authors have explained security issues on mobile cloud applications and related to private data .

By knowing the security issues and existing solutions limitation, The author proposed a mobile computing application security framework to make sure that data security is gained when it is transferred between the same mobile application. The architecture also identifies that the integrity of the application at the time of installation or updation on the mobile device is complete. The framework in the Saas layer of the cloud service delivery model provides the security service like integrity and confidentiality. The author in [9] have highlighted the architecture of MCC .The application of MCC is explained such as mobile commerce ,mobile learning ,mobile games. The author also proposed issues like low bandwidth ,Network access management, quality of service ,standard interface.

The author[10] explains the existing solution to secure MCC infrastructure and also clearly explained the uprising issues in MCC The secure cloud physical services are applicable at the backbone layer. Secure cloud process hosting services are available at the infrastructure and supervisor layers .

The author in [11] have come-out with a mobile computing architecture and introduced various methods to implement MCC effectively and efficiently. They also discussed about the critical issues and challenges available in MCC. The authors have the MCC solutions into two different ways. The first way, a system is developed which have the same cloud structure which is used by users in the need to improve the performance of mobile devices and in the second way, which has different applications for mobile devices which uses cloud computing. The second way is best for email or chatting why because ,internet used as a common resource in device instead of storage.

MCC has barriers for shifting from cloud computing to mobile computing. The barriers are Saas is implemented in MCC for the reason of limited storage ,less battery, poor display and less computational power of mobile device, No proper standard ,This leads to problem like limited scalability, unreliable of service and service provider lock-in. There are two various types of services in security proposed by the author of[12].They are Critical security service(CSS), Normal Security service(NSS).The critical security service holds more cloud resources and also provide good security and protection those CSS offers reward to the cloud service providers. The goal of Security service Admission Model(SSAM) is to allocate cloud resources efficiently to a large numbers of Critical Security(CS) and Normal Security(NS) service users. The SSAM is purely based upon Semi-Markov decision process in order to utilize system resource efficiently and also to increase the system reward for cloud service providers. The SSAM drives blocking probability of the cloud service and obtain maximum system increase by keeping system expenses and rewards in mobile cloud infrastructure.

In [13] a method to improve security of cloud computing is introduced. the method is based upon dynamic intrusion detection system which send its detectors which resides on the networking system domain through multi layers and multistage deployment. This method ensures wide range of security protection like protecting websites and pages threats, verifying the database access and also the security in cloud side and some other issues related to processes.A new trendy mobile computing framework proposed by author in [14]which provides the functionality of traditional computation service.

Its main aim is to increase the working of mobile and ad-hoc network respect to trust and risk management and also routing in protected way. After these enhancement made in traditional mobile ad-hoc network (MANET) model is changed to a new service oriented model. This new model view every mobile node as a service node. The capability of the service node and the services it offer and use are directly proportional to each other .The services have a wide range and they will be storage ,sensing or computational services. To decrease the concern enhanced by the mobility ,some Extended Semi Shadow Image (ESSI) are mirrored on cloud. The ESSI can be a copy or image of the devices which hold more resources with enhanced functionality .To provide secure communication, the ESSI and mobile node uses Secure Socket Layer(SSL),Internet Protocol Security(IPSec) etc.

III. PROPOSED WORK

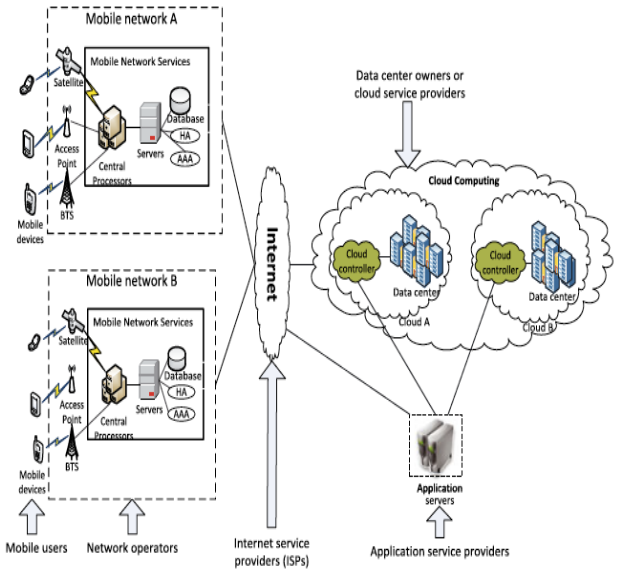


FIGURE 2

Above architecture can be implemented to improve security. Access point (Base station) used to connect mobile phones to the mobile networks and also it acts as an intermediate between the mobile phones and the mobile network. Access point is responsible for establishing the connection and managing connection between them. The requested information and the details of the user are transferred to centralized processor which in turn connected to the server, is responsible for providing the network services .Based upon the subscriber's data stored on the database ,network operators provide services to users after the authorization and authentication is done .once the user request is sent to cloud through internet ,the cloud controllers responds to the mobile users by providing appropriate cloud services.

These services include the methodology of utility computing ,virtualization and service oriented architecture (e.g. web application, data base servers)MCC is growing day by day due to the efficiency of cloud computing .security is the major challenge in MCC because the mobile users data's or files are more sensitive and confidential .MCC must provide a security in such a way that any unauthorized harm the data stored on the cloud. Application models or mobile application should be protected to provide better services to the mobile users by consuming the cloud resources .The services of the cloud are used by the application model in order to increase the capability of the mobile devices.The restrictions and limitations of mobile devices and the wireless network are the major challenges of mobile cloud computing which makes the application designing ,deploying a mobile and distributed devices more complicated than on the fixed cloud devices. The factors that affects the assessing from cloud computing are limitations of mobile devices, quality of wireless communication, types of application, and support from cloud computing to mobile

CHALLENGES	SOLUTIONS
Limitation of mobile devices	Virtualization and Image Task migration.
Quality of communication	Bandwidth upgrading, Data delivery time reducing.
Division of applications services	Elastic application division mechanism

TABLE 1: CHALLENGES AND SOLUTIONS OF MCC

A. DATA STORAGE SECURITY WITH VARIOUS AVAILABLE SOLUTIONS

For the last few years Mobile Cloud Computing has been an active research field, as mobile cloud computing is in initial stage, limited surveys are available in various domain of MCC. In this paper our main focus is on securing the data storage in mobile cloud computing. Significant efforts have been devoted in research organizations to build secure mobile cloud computing. This paper explores the various methodologies for data security in Mobile Cloud Computing. proposed an Energy efficient framework for integrity verification of storage services using incremental cryptography and trusted computing.

In this paper the authors provided a framework for mobile devices to provide data integrity for data stored in cloud server. Incremental cryptography has a property that when this algorithm is applied to a document, it is possible to quickly update the result of the algorithm for a modified document, rather than to re-compute it from scratch. In this system design three main entities are involved Mobile User (MU): Mobile user/client is a person who utilizes the storage services provided by Cloud service provider (CSP).Cloud Service Provider (CSP): CSPprovides storage services to client. CSP is also responsible for operating, managing and allocating cloud resources efficiently. Trusted Third Party (TTP): TTP installs coprocessors on remote cloud; who is associated with a number of registered mobile user/client. Coprocessor provides secretkey (SEK) to mobile user and is also responsible for generating message authentication code for mobile client. There are a number of operations involved in this scheme shown by

1. Updating File on the Cloud: Before uploading file on cloud, mobile user is required to generate an incremental Message Authentication Code (MAC file) using SEK.
MACfile = Σ HMAC (Filek , SEK). (1)Where, n is total logical partitions of file and Filek is kth part of the file.

After generating MAC file, mobile client uploads the file on the cloud and stores MAC file on local storage.

2. Inserting or deleting a block*:*

At any time mobile client can insert (delete) a data block in file stored on cloud server. For this client sends request to CSP, in its response CSP sends requested file to mobile client as well as to trusted coprocessor (TCO) associated with that client. TCO generates MACtco and sends it to client to match this MAC generated by TCO (MACtco) with MAC stored in client's local storage (MACfile). If these two MAC matches , the client can perform insertion/deletion in the file and again computes MACfile with help of old MACfile, SEK and inserted/deleted block. For avoiding communication overhead only updated block is uploaded on cloud server.3) Integrity Verification: At any time mobile client can verify the integrity of data stored on cloud server by sending request to cloud server, on receiving request cloud server sends file to TCO for integrity verification. TCO generates incremental authentication code and sends it to mobile client directly. Now mobile client compares this MACtco with stored MACfile to verify integrity. If these two matches then integrity is verified BY.

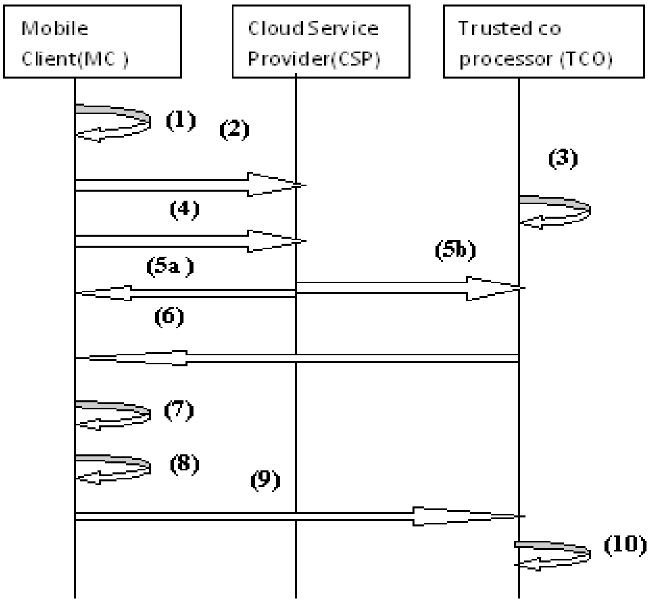


FIGURE 3:Communication between the MC,CSP,TCO[5]

THE FOLLOWING PSEUDOCODE

PSEUDOCODE: Integrity verification

```
Step1   : MC generate MACfile and stores MACfile in local
          Memory
Step 2  : MC uploads file on server
Step 3  : CSP stores file on cloud
Step 4  : MC sends request to CSP for performing
          insertion/deletion in the file
Step 5a : CSP sends requested file to MC
Step 5b : CSP forwards requested file to TCO
Step 6  : TCO sends MACtco to MC directly
Step7   : MC compares MACfile and MACtco for verifying
          integrity
Step8   : MC insert/delete a block in file and computes
          MAC for that block
Step 9  :MC uploads updated block on cloud
Step 10 :CSP stores updated file.
```

The proposed approach consists of following two steps

B. CLOUDBASED CLIENT-SERVER ARCHITECTURE

The client-server architecture is required in the initial level of mobile cloud computing .The client side is the applications which are present in the smart phone .The connection must be established with the server where the data is to be uploaded and downloaded .The network connection may be LAN /WAN based upon the server which provides cloud services

IV. SECURITY FEATURES

The client-server architecture must be secured or protected by using a particular algorithm. The dynamic security is provided by the symmetric key oriented algorithm. The MAC Address of every device is unique so that it (devices) can be cross verified to improve the security level. The unique MAC address finds the correct device using cloud applications A set of specially derived keys (round keys) are required for the encryption process. These are used along with several operations on an array that contains only one block of data to be encrypted.

ENCRYPTION ALGORITHM

```
Input   : A set contains plain text (data)
Output:  set of Encrypted data (cipher text)
Method: The following steps are used to encrypt a block
which contains 128 bits
Step1   : create the set of keys called round key from the
Cipher key
Step2   : Initialize the state array with plain text or data
Step 3  : Add the first round key to the starting array
Step4   : perform state manipulation with nine rounds
Step 5  : perform tenth and last round of state
Manipulation
Step6   : assign the last state array as encrypted
          data (cipher text)
```

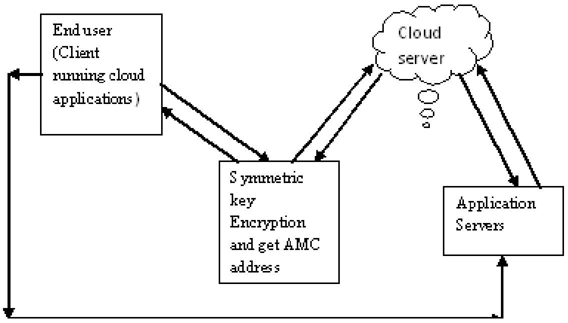

End user (Client running cloud applications)
Cloud server
Symmetric key Encryption and get AMC address
Application Servers

FIGURE 4:Symmetric key Encrption method

Here tenth rounds performs little different manipulation from the other rounds. The above algorithm encrypts the block of 128 bits. Initially the 128 bits (1 block) is converted into 16 bytes and operations are performed based on the two -dimensional array (state array)which is a byte array having four rows and four columns . The 16 bytes are numbered from B0 to B15 are stored into that array. This array is modified during each round of encryption which requires the following sequence of steps.

SubBytes: non-linear substitution step where each byte is replaced with another according to a lookup table.

ShiftRows: a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

MixColumns: a mixing operation which operates on the columns of the state, combining the four bytes in each column.

Add round key: each byte of the state is combined with a block of the round key using bitwise XOR.

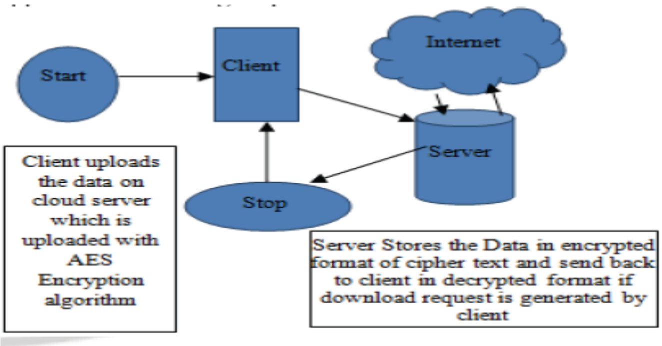
Decryption process involves the following inverse functions.The functions are InvSubBytes, InvShiftRow, InvMixColumns ,XorRoundKey which doesn't need an inverse function because XORing twice will give the original value. InvSubBytes works the same way as SubBytes but uses a different table that returns the original value. InvShiftRows does the rotating of left instead of right and InvMixColumns uses a various constant matrix to multiply the co lumns.

DECRYPTION ALGORITHM

Input : Encrypted data(cipher text)
Output: Original data(Plaintext)
Method: The order of operation in decryption is:

```
Step1: Perform initial decryption round:
        XorRoundKey
        InvShiftRows
        InvSubBytes
Step2: Perform nine full decryption rounds:
        XorRoundKey
        InvMixColumns
        InvShiftRows
        InvSubBytes
Step3:Perform final XorRoundKey
```

The same round keys are used in the same order


Start
Client
Internet
Server
Stop
Client uploads the data on cloud server which is uploaded with AES Encryption algorithm
Server Stores the Data in encrypted format of cipher text and send back to client in decrypted format if download request is generated by client

The above diagram explains the flow of proposed system which is been developed for MCC client-server architecture. The mobile users can upload the confidential information on the cloud server. The uploaded data in the cloud is secured through the above encryption algorithm. For highest protection we have added a technique of MAC address verification which identifies the exact user during authentication. The MAC address of a mobile user is taken during the sign up process stored into database and this MAC address is verified in order to ensure the exact user whenever the users logged on to the cloud .If MAC address is matched the user of application is a genuine owner. If it doesn't matches the application will not get opened.

REFERENCES

[1] Portio Research,"Mobile subscribers worldwide," http://www.onbile.com/info/mobile-subscribers-worldwide.
[2] Hoang T. Dinh, Chonho Lee, Dusit Niyato and Ping Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," Wirel. Commun. Mob. Comput. ,2011.
[3] A Survey of Mobile Cloud Computing:Architecture, Applications, and Approaches by Hoang T. Dinh, Chonho Lee, Dusit Niyato.
[4] M. Al Morsy, J. Grundy and I. Müller, "An Analysis of The Cloud Computing Security Problem", In Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, (**2010**), November 30.
[5] Soeung-Kon, J. -H. Lee and S. W. Kim, "Mobile Cloud Computing Security Considerations", Journal of Security Engineering, no. 9, (**2012**) April
[6] K. opovi and Z. Hocenski, "Cloud computing security issues and challenges", MIPRO, 2010 Proceedings of the 33rd International Convention, (**2010**) May 24-28.
[7] D. Chen and H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", International Conference on Computer Science and Electronics Engineering (ICCSEE), (**2012**) March 23-25.
[8] D. Popa, M. Cremene, M. Borda and K. Boudaoud, "A security framework for mobile cloud applications", 11th Roedunet International Conference (RoEduNet), (**2013**) January 17-19.
[9] H. T. Dinh, C. Lee, D. Niyato and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches", Wireless Communications and Mobile Computing - Wiley, (**2011**) October.
[10] A. N. Khana, M. L. M. Kiaha, S. U. Khanb and S. A. Madanic, "Towards secure mobile cloud computing: A survey", Future Generation Computer Systems, vol. 29, Issue 5, (**2013**) July
[11] S. S. Qureshi, T. Ahmad, K. Rafique and Shuja-ul-islam, "Mobile cloud computing as future for mobile applications – Implementation methods and challenging issues", IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS), (**2011**) September 15-17.
[12] H. Liang, D. Huang, L. X. Cai, X. Shen and D. Peng, "Resource Allocation for Security Services in Mobile Cloud Computing", IEEE Infocom 2011 Workshop on M2MCN, (**2011**).
[13] C. -L. Tsai, U. -C. Lin, A. Y. Chang and C. -J. Chen, "Information

INTERNET OF THINGS FOR SMART CITIES

M.G.Vishal kumaar#1 , N.D.V Sricharan*2 , X.Shibin*3 , Mr. M. B. Prasanth Yokesh*4

1,2,3UG Student, Department of Computer Science & Engineering, Anand Institute of Higher Technology, Kazhipattur, Chennai.

*4Assistant Professor, Department of Computer Science & Engineering, Anand Institute of Higher Technology, Kazhipattur, Chennai.

vishal.kumaar123@gmail.com

***Abstract* - The Internet of Things (IoT) shall be able to incorpo- rate transparently and seamlessly a large number of different and heterogeneous end systems, while providing open access to selected subsets of data for the development of a plethora of digital services. Building a general architecture forthe IoT is hence a very complex task, mainly because of the extremely large variety of devices, link layer technologies, and services that may be involved in such a system. In this paper, we focus specifically to an urban IoT system that, while still being quite a broad category, are characterized by their specific application domain. Urban IoTs, in fact, are designed to support the Smart City vision, which aims at exploiting the most advanced communication technologies to support added-valueservices for the administration of the city and for the citizens. This paper hence provides a comprehensive survey of the enabling technologies, protocols, and architecture for an urban IoT. Fur- thermore, the paper will present and discuss the technical solutions and best-practice guidelines adopted in the Padova Smart City project, a proof-of-concept deployment of an IoT island in the city of Padova, Italy, performed in collaboration with the city municipality.**

***Index Terms*—Constrained Application Protocol (CoAP), Efficient XML Interchange (EXI), network architecture, sensor system integration, service functions and management, Smart Cities, testbed and trials, 6lowPAN.**

I.INTRODUCTION

Everyday life will be equipped with microcontrollers, transceivers for digital communication, and suitable protocol stacks that will make them able to communicate with one another and with the users, becoming an integral part of the Internet. The IoT concept, hence, aims at making the Internet even more immersive and pervasive. Furthermore, by enabling easy access and interaction with a wide variety of devices such as, for instance, home appliances, surveillance cameras, monitoring, however, such a heterogeneous field of application makes the identification of solutionscapable of satisfying the requirements of all possible application scenarios a formidable challenge.
This dificulty has led to the proliferation of different and, sometimes, incompatible proposals for the practical realization of IoT systems. Therefore, from a system perspective, the realization of an IoT network, together with the required backend network ser-vices and devices, still lacks an established best practice because of its novelty and complexity.In addition to the technical difficulties, the adoption of the IoT paradigm is also hindered by the lack of a clear and widely accepted business model that can attract investments to promote the deployment of these technologies.

In this complex scenario, the application of the IoT paradigm to an urban context is of particular interest, as it responds to the strong push of many national governments to adopt ICT solutions in the management of public affairs, thus realizing the so- called Smart City concept s. Although there is not yet a formal and widely accepted definition of “Smart City,” the final aim is to make a better use of the public resources, increasing the quality of the services offered to the citizens, while reducing the operational costs of the public administrations. This objective can be pursued by the deployment of an urban IoT, i.e., a communication infrastructure that provides unified, simple, andeconomical access to a plethora of public services, thus unleashing potential synergies and increasing transparency to the citizens. An urban IoT, indeed, may bring a number of benefits in the management and optimization of traditional public services, such as transport and parking, lighting, surveillance and maintenance of public areas, preservation of cultural heritage, garbage collection, salubrity of hospitals, and school.

Furthermore, the availability of different types of data, collected by a pervasive urban IoT, may also be exploited to increase the transparency and promote the actions of the local government toward the citizens, enhance the awareness of people about the status of their city, stimulate the active participation of the citizens in the management of public administration, and also stimulate the creation of new services upon those provided by the IoT
Therefore, the application of the IoT paradigm to the Smart City is particularly attractive to local and regional administrations that may become the early adopters of such technologies, thus acting as catalyzers for the adoption of the IoT paradigm on a wider scale

II. SMART CITY CONCEPT AND SERVICES|

According to Pike Research on Smart Cities, the Smart City market is estimated at hundreds of billion dollars by 2020, with an annual spending reaching nearly
16 billion. This market springs from the synergic interconnection of key industry and sectors, such as Smart Governance, Smart Mobility, Smart Utilities, Smart Buildings, and Smart Environment. These sectors have also been considered in the European Smart Cities project (http://www.smart-cities.eu) to define a ranking criterion that can be used to assess the level of “smartness” of European cities. Nonetheless, the Smart City market has not really taken off yet, for a number of political, technical, and

financial barriers. Under the political dimension, the primary obstacle is the attribution of decision-making power to the different stake- holders. A possible way to remove this roadblock is to institutionalize the entire decision and execution process, concentrating the strategic planning and management of the smart city aspects into a single, dedicated department in the city .

On the technical side, the most relevant issue consists in the non-interoperability of the heterogeneous technologies currently used in city and urban development. In this respect, the IoT vision can become the building block to realize a unified urban- scale ICT platform, thus unleashing the potential of the Smart City vision.

In the rest of this section, we overview some of the services that might be enabled by an urban IoT paradigm and that are of potential interest in the Smart City context because they can realize the win–win situation of increasing the quality and enhancing the services offered to the citizens while bringing an economical advantage for the city administration in terms of reduction of the operational costs [6].

Structural Health of Buildings: Proper maintenance of the historical buildings of a city requires the continuous monitoring of the actual conditions of each building and identification of the areas that are most subject to the impact of external agents. The urban IoT may provide a distributed database of building structural integrity measurements, collected by suitable sensors located in the buildings, such as vibration and deformation sensors to monitor the building stress, atmospheric agent sensors in the surrounding areas to monitor pollution levels, and temperature and humidity sensors to have a complete characterization of theenvironmental conditions. This database should reduce the need for expensive periodic structural testing by human operators and will allow targeted and proactive maintenance and restoration actions. Finally, it will be possible to combine vibration and seismic readings in order to better study and understand the impact of light earthquakes on city buildings. This database can be made publicly accessible in order to make the citizens aware of the care taken in preserving the city historical heritage. The practical realization of this service, however, requires the installation of sensors in the buildings and surrounding areas and their interconnection to a control system, which may require an initial investment in order to create the needed infrastructure.

Waste Management: Waste management is a primary issue in many modern cities, due to both the cost of the service and the problem of the storage of garbage in land fills. A deeper penetration of ICT solutions in this domain, however, may result in significant savings and economical and ecological advantages. For instance, the use of intelligent waste containers, which detect the level of load and allow for an optimization of the collector trucks route, can reduce the cost of waste collection and improve the quality of recycling. To realize such a smart waste management service, the IoT shall connect the end devices, i.e., intelligent waste containers, to a control center where an optimization software processes the data and determines the optimal management of the collector truck fleet.

Traffic Congestion: On the same line of air quality and noise monitoring, a possible Smart City service that can be enabled by urban IoT consists in monitoring the traffic congestion in the city. Even though camera-based traffic monitoring systems are already available and deployed in many cities, low-power widespread communication can provide a denser source of information. Traffic monitoring may be realized by using the sensing capabili- ties and GPS installed on modern vehicles, and also adopting a combination of air quality and acoustic sensors along a given road. This information is of great importance for city authorities and citizens: for the former to discipline traffic and to send officers where needed and for the latter to plan in advance the route to reach the office or to better schedule a shopping trip to the city centre.

City Energy Consumption: Together with the air quality monitoring service, an urban IoT may provide a service to monitor the energy consumption of the whole city, thus enabling authorities and citizens to get a clear and detailed view of the amount of energy required by the different services (public lighting, transportation, traffic lights, control cameras, heating/cooling of public buildings, and so on). In turn, this will make it possible to identify the main energy consumption sources and to set priorities in order to optimize their behavior. This goes in the direction indicated by the European directive for energy eficiency improvement in the next years. In order to obtain such a service, power draw monitoring devices must be integrated with the power grid in the city. In addition, it will also be possible to enhance these service with active functionalities to control local power production structures (e.g., photovoltaic panels).

Smart Parking: The smart parking service is based on road sensors and intelligent displays that direct motorists along the best path for parking in the city . The beneit deriving from this service are manifold: faster time to locate a parking slot means fewer CO emission from the car, lesser traficongestion, and happier citizens. The smart parking service can be directly integrated in the urban IoT infrastructure, because many companies in Europe are providing market products for this application. Furthermore, by using short-range communication technologies, such as Radio Frequency Identiir(RFID) or Near Field Communication (NFC), it is possible to realize an electronic veriiainsysemof parking permits in slots reserved for residents or disabled, thus offering a better service to citizens that can legitimately use those slots and an efiintooltoquickly spot violations.Smart Lighting: In order to support the 20-20-20 directive, the optimization of the street lighting eficiency is an important feature. In particular, this service can optimize the street lamp intensity according to the time of the day, the weather condition, and the presence of people. In order to properly work, such a service needs to include the street lights into the Smart City infrastructure. It is also possible to exploit the increased number of connected spots to provide Wi-Fi connection to citizens. In addition, a fault detection system will be easily realized on top of the street light controllers.

III. URBAN IOT ARCHITECTURE

From the analysis of the services described in Section II, it clearly emerges that most Smart City services are based on a centralized architecture, where a dense and heterogeneous set of peripheral devices deployed over the urban area generate different types of data that are then delivered through suitable com munication technologies to a control center, where data storage and processing are performed.A primary characteristic of an urban IoT infrastructure, hence, is its capability of integrating different technologies with the existing communication infrastructures in order to support a progressive evolution of the IoT, with the interconnection of other devices and the realization of novel functionalities and services. Another fundamental aspect is the necessity to make (part of) the data collected by the urban IoT easily accessible by authorities and citizens, to increase the responsiveness of authorities to city problems, and to promote the awareness and the participation of citizens in public matters.

In the rest of this section, we describe the different components of an urban IoT system, as sketched in Fig. 1. We start describing the web service approach for the design of IoT services, which requires the deployment of suitable protocol layers in the differ- ent elements of the network, as shown in the protocol stacks

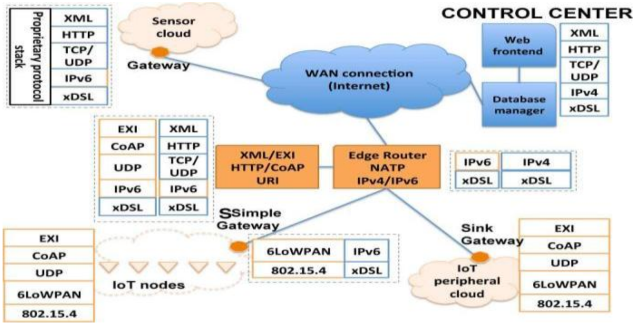


Fig.1. Conceptual representation of an urban IoT network based on the web service approach.

Although in the IoT domain many different standards are still struggling to be the reference one and the most adopted, in this section we focus speciiayon IETF standards because they are open and royalty-free, are based on Internet best practices, and can count on a wide community.

1)Integration of multiple XML/EXI data sources into an IoT system can be obtained by using the databases typically created and maintained by high-level applications. In fact, IoT applications generally build a database of the nodes controlled by the application and, often, of the data generated by such nodes. The database makes it possible to integrate the data received by any IoT device to provide the speciic service the application is built for. A generic framework for building IoT web applications according to the guidelines described in this section has been proposed in, where the authors also suggest exploiting the Asynchronous JavaScript and XML (AJAX) capabilities of modern web browsers that allow for a direct communication between the browser and the ial IoT node, demonstrating the full internetworking of the protocol stack and the open data nature of the proposed approach.

2) APPLICATION AND TRANSPORT LAYER: Most of the trafcthat crosses the Internet nowadays is carried at the application layer by HTTP over TCP. However, the verbosity and complexity of native HTTP make it unsuitable for a straight deployment on constrained IoT devices. For such an environment, in fact, the human-readable format of HTTP, which has been one of the reasons of its success in traditional networks, turns out to be a limiting factor due to the large amount of heavily correlated (and, hence, redundant) data. Moreover, HTTP typically relies upon the TCP transport protocol that, however, does not scale well on constrained devices, yielding poor performance for small data flows in lossy environments.

3) Network Layer: IPv4 is the leading addressing technology supported by Internet hosts. However, IANA, the international organization that assigns IP addresses at a global level, has recently announced the exhaustion of IPv4 address blocks. IoT networks, in turn, are expected to include billions of nodes, each of which shall be (in principle) uniquely addressable. A solution to this problem is offered by the IPv6 standard [24], which provides a 128-bit address field, thus making it possible to assign a unique IPv6 address to any possible node in the IoT network.

An urban IoT system, due to its inherently large deployment area, requires a set of link layer technologies that can easily cover a wide geographical area and, at the same time, support a possibly large amount of traffic resulting from the aggregation of an extremely high number of smaller data flows. For these reasons, link layer technologies enabling the realization of an urban IoT system are classified into unconstrained and constrained technologies. The first group includes all the traditional LAN, MAN, and WAN communication technologies, such as Ethernet, Wi-Fi, fiber optic, broadband Power Line Communication (PLC), and cellular technologies such as UMTS and LTE. They are generally characterized by high reliability, low latency, and high transfer rates (order of Mbit/s or higher), and due to their inherent complexity and energy consumption are generally not suitable for peripheral IoT nodes.

IV. AN EXPERIMENTAL STUDY: PADOVA SMART CITY

The framework discussed in this paper has already been successfully applied to a number of different use cases in the context of IoT systems. For instance, the experimental wireless sensor network testbed, with more than 300 nodes, deployed at the University of Padova has been designed according to these guidelines, and successfully used to realize proof-of- concept demonstrations of smart grid [33] and health care services.

The primary goal of Padova Smart City is to promote the early adoption of open data and ICT solutions in the public adminis- tration. The target application consists of a system for collecting environmental data and monitoring the public street lighting by means of wireless nodes, equipped with different kinds of sensors, placed on street light poles and connected to the Internet through a gateway unit. This system shall make it possible to collect interesting environmental parameters, such as CO level, air temperature and humidity, vibrations, noise, and so on, while providing a simple but accurate mechanism to check the correct operation of the public lighting system by measuring the light intensity at each post. Even if this system is a simple application of the IoT concept, it still involves a number of different devices and link layer technologies, thus being representative of most of the critical issues that need to be taken care of when designing an urban IoT. A high-level overview of the types and roles of the devices involved in the system is given hereafter.

Database server: The database server collects the state of the resources that need to be monitored in time by communicating with the HTTP CoAP proxy server, which in turn takes care of retrieving the required data from the proper source. The data stored in the database are accessible through traditional web programming technologies. The information can either be visualized in the form of a web site, or exported in any open data format using dynamic web programming languages. In the Padova Smart City network, the database server is realized within the WSN Gateway, which hence represents a plug- and-play module that provides a transparent interface with the peripheral nodes. Operator mobile device: Public lighting operators will be equipped with mobile devices that can locate the streetlight that requires intervention, issue actuation commands directly to the IoT node connected to the lamp, and signal the result of the intervention to the central system that can track every single lamppost and hence, optimize the maintenance plan.

V. CONCLUSION

In this paper, we analyzed the solutions currently available for the implementation of urban IoTs. The discussed technologies are close to being standardized, and industry players are already active in the production of devices that take advantage of these technologies to enable the applications of interest, such as those described in Section II. In fact, while the range of design options for IoT systems is rather wide, the set of open and standardized protocols is significantly smaller. The enabling technologies, furthermore, have reached a level of maturity that allows for the practical realization of IoT solutions and services, starting from field trials that will hopefully help clear the uncertainty that still prevents a massive adoption of the IoT paradigm

REFERENCE

[1] L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” Comput. Netw., vol. 54, no. 15, pp. 2787–2805, 2010.

[2] P. Bellavista, G. Cardone, A. Corradi, and L. Foschini, “Convergence of MANET and WSN in IoT urban scenarios,” IEEE Sens. J., vol. 13, no. 10, pp. 3558–3567, Oct. 2013.

[3] A. Laya, V. I. Bratu, and J. Markendahl, “Who is investing in machine- to- machine communications?” in Proc. 24th Eur. Reg. ITS Conf., Florence, Italy, Oct. 2013, pp. 20–23.

[4] H. Schaffers, N. Komninos, M. Pallot, B. Trousse, M. Nilsson, and A. Oliveira, “Smart cities and the future internet: Towards cooperation fram eworks for open innovation,” The Future Internet, Lect. Notes Comput. Sci., vol. 6656, pp. 431–446, 2011.

[5] D. Cuff, M. Hansen, and J. Kang, “Urban sensing: Out of the woods,” Commun. ACM, vol. 51, no. 3, pp. 24–33, Mar. 2008.

[6] M. Dohler, I. Vilajosana, X. Vilajosana, and J. Llosa, “Smart Cities: An action plan,” in Proc. Barcelona Smart Cities Congress Barcelona, Spain, Dec. 2011, pp. 1–6.

BIG BANK VIRTUALIZATION BIG DATA WITH CLOUD VIRTUALIZATION FOR EFFECTIVE RESOURCE HANDLING

S.Parthasarathy [#1], N.Sathyajithray [*2] B.Vinoth Kumar [*3], Mrs. Mary Joseph [*4]

[#1,*2, *3] *UG Student, Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai.*

[*4] *Professor, Department of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai.*

parthasarathy2304@gmail.com

Abstract— **In the system, Integration of Cloud & Big Data is the most challenging task to handle. Further addition of Virtualization is implemented for effective data Processing. Integration of Big Data & Cloud s achieved. Virtual Machines can be added or removed as per the request. This process assures QOS for Clients.We deploy Two Clouds for handling 4 Jobs like Credit Card, Loan, ATM and Direct Banking. We develop this Application for banking. We also achieve Virtualization in our Local Machine. We can add or remove VMs in those machines. Based on the number of request the main Cloud Server will add the VMs or remove the VMs. There will be minimum one VM and maximum 3 VMs are assigned per Server.**

***Index Terms*—QOS, Virtualisation, BigData**

I. INTRODUCTION

CLOUD computing assembles large networks of virtualized ICT services such as hardware resources (such as CPU, storage, and network), software resources (such as databases, application servers, and web servers) and applications. In industry these services are referred to as infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Mainstream ICT powerhouses such as Amazon, HP, and IBM are heavily investing in the provision and support of public cloud infrastructure. Cloud computing is rapidly becoming a popular infrastructure of choice among all types of organizations. Despite some initial security concerns and technical issues, an increasing number of organizations have moved their applications and services in to “The Cloud”. These applications range from generic word processing software to online healthcare. The cloud system taps into the processing power of virtualized computers on the back end, thus significantly speeding up the application for the user, which just pays for the used services. Big Data applications has become a common phenomenon in domain of science, engineering, and commerce. Some of the representative applications include disaster management, high energy physics, genomics, connectomics, automobile simulations, medical imaging, and the like. The “Big Data” problem, which is defined as the practice of collecting and analyzing complex data sets so large that it becomes difficult to analyze and interpret manually or using on-hand data management applications (e.g., Microsoft Excel). ”. These applications range from generic word processing software to online healthcare. The cloud system taps into the processing power of virtualized computers on the back end, thus significantly speeding up the application for the user, which just pays for the used services.

II.*BASICS OF CLOUD COMPUTING*

CLOUD computing assembles large networks of virtualized ICT services such as hardware resources (such as CPU, storage, and network), software resources (such as databases, application servers, and web servers) and applications. In industry these services are referred to as infra- structure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Mainstream ICT power- houses such as Amazon, HP, and IBM are heavily investing in the provision and support of public cloud infrastructure. Cloud computing is rapidly becoming a popular infrastructure of choice among all types of organizations. Despite some initial security concerns and technical issues, an increasing number of organizations have moved their applications and services in to “The Cloud”. These applications range from generic word processing software to online healthcare. The cloud system taps into the processing power of virtualized computers on the back end.

III.APPLICATION OF BIGDATA

Big Data applications has become a common phenomenon in domain of science, engineering, and commerce. Some of the representative applications include disaster management, high energy physics, genomics, connectomics, automobile simulations, medical imaging, and the like. The “Big Data” problem, which is defined as the practice of collecting and analyzing complex data sets so large that it becomes difficult to analyse and interpret manually or using on-hand data management applications (e.g., Microsoft Excel).

For example, in case of disaster management Big Data application there is a need to ana- lyse “a deluge of online data from multiple sources (feeds from social media and mobile devices)” for under-standing and managing real-life events such as flooding,earthquake, etc. Over 20 million tweets posted during Hurricane Sandy (2012) lead to an instance of the BigData problem. The statistics provided by the PearAnalytics study reveal that almost 44 percent of the Twitter posts are spam and pointless, about 6 percent are personal or product advertising, while

3.6 percent are news and 37.6 percent are conversational posts.

During the 2010 Haiti earthquake, text messaging via mobile phones and Twitter made headlines as being crucial for disaster response, but only some 100,000 messages were actually processed by government agencies due to lack of auto- mated and scalable ICT (cloud) infrastructure.

Large-scale, heterogeneous, and uncertain Big Data applications are becoming increasingly common, yet current cloud resource provisioning methods do not scale well and nor do they perform well under highly unpredictable conditions (data volume, data variety, data arrival rate, etc.).

Much research effort have been paid in the fundamental understanding, technologies, and concepts related to autonomic provisioning of cloud resources for Big Data applications, to make cloud-hosted Big Data applications operate more efficiently, with reduced financial and envi- ronmental costs, reduced underutilization of resources, and better performance at times of unpredictable workload.

Targeting the aforementioned research challenges, this special issue compiles recent advances in Autonomic Provisioning of Big Data Applications on Clouds.

IV.VIRTUALIZATION

Virtualized clouds introduce performance variability in resources, thereby impacting the application's ability to meet its quality of service(QoS). This motivates the need for autonomic methods of provisioning elastic resources as well as dynamic task selection, for continuous dataflow applications on clouds. Kumbhare et al. extend continuous dataflows to the concept of "dynamic dataflows", which utilize alternate tasks definitions and offer additional control over the dataflow's cost and QoS. They formalize an optimization problem to automate both deploy ment time and runtime cloud resource provisioning of such dynamic dataflows that allows for trade-offs between the application's value and the resource cost. They propose two greedy heuristics, centralized and shared, based on the variable sized bin packing algorithm to solve this NP-hard problem. Further, they also present a genetic algorithm (GA) metaheuristic that gives a near optimal solution by exploring a wide range of possible configurations.Elasticity has now become the elemental feature of cloud computing as it enables the ability to dynamically add or remove virtual machine instances when workload changes. However, effective virtualized resource management is still one of the most challenging tasks. When the workload of a service increases rapidly, existing approaches cannot respond to the growing performance requirement efficiently because of either inaccuracy of adaptation decisions or the slow process of adjustments, both of which may result in insufficient resource provisioning. As a consequence, the QoS of the hosted applications may degrade and the service level objective (SLO) will be thus violated. Liu et al. introduce SPRNT, a novel resource management framework, to ensure high-level QoS in the cloud computing sys- tem. SPRNT utilizes an aggressive resource provisioning strategy which encourages SPRNT to substantially increase the resource allocation in each adaptation cycle when workload increases.

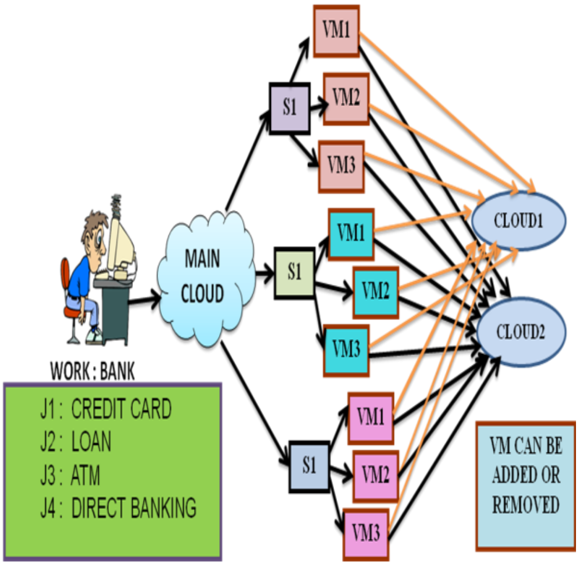
V.DEVELOPMENT TECHNIQUES(CLOUD)

The scheduling of multitask jobs on clouds is an NP- hard problem. The problem becomes even worse when complex workflows are executed on large elastic clouds, such as Amazon EC2 or IBM RC2. The main difficulty lies in the large search space and high overhead for generation of optimal schedules, especially for real-time applications with dynamic workloads. A new iterative ordinal optimization (IOO) method is proposed by Zhang et al. The ordinal optimization method is applied in each iteration to achieve suboptimal schedules. IOO aims at generating more efficient schedules from a global perspective over a long period. They prove through overhead analysis the advantages in time and space efficiency in using the IOO method. The IOO method is designed to adapt to system dynamism to yield suboptimal performance.As cloud computing makes computing a utility, scientists across different application domains are facing the same challenge of reducing financial cost in addition to meet the traditional goal of performance optimization. Wu et al. develop a prototype generic workflow system by leveraging existing technologies for a quick evaluation of scientific workflow optimization strategies.

They construct analytical models to quantify the network performance of scientific work- flows using cloud-based computing resources, and formulate a task scheduling problem to minimize the workflow end-to-end delay under a user-specified financial constraint.Despite recent efforts toward designing resource- efficient MapReduce schedulers for large-scale cloud applications, existing solutions that focus on scheduling at the task-level still offer sub-optimal job performance. This is because tasks can have highly varying resource requirements during their lifetime, which makes it difficult for task-level schedulers to effectively utilize available resources to reduce job execution time. To address this limitation, Zhang et al. introduce PRISM, a fine-grained resource-aware MapReduce scheduler that divides tasks into phases, where each phase has a constant resource usage profile, and performs scheduling at the phase level.

VI.MODIFICATION SYSTEM

The modification is our Implementation. We deploy Two Clouds for handling 4 Jobs like Credit Card, Loan, ATM and Direct Banking. We develop this Application for banking. We also achieve Virtualization in our Local Machine. We can add or remove VMs in those machines. Based on the number of request the main Cloud Server will add the VMs or remove the VMs. There will be minimum one VM and maximum 3 VMs are assigned per Server.



VII.ADVANTAGES

- Less time consumption
- High data transmission rate
- More effective

VIII.CONCLUSION

In large-scale cloud computing application domains, propose a secure cloud computing based framework for big data information management in smart grids, which is called "Smart-Frame." The main idea of our framework is to build a hierarchical structure of cloud computing centers to provide different types of computing services for information management and big data analysis. In addition to this structural framework, they present a security solution based on identity-based encryption, signature and proxy re-encryption to address critical security issues of the proposed framework.

REFERENCES

[1] Cloud Computing: Methodology, Systems, and Applications, L. Wang, R. Ranjan, J. Chen, and B. Benatallah Eds. Boca Raton, FL: CRC Press, Taylor and Francis Group, p. 844, Oct. 2011.

[2] R. Pepper and J. Garrity, "The internet of everything: How the network unleashes the benefits of big data," CISCO [Online]. Available: http://blogs.cisco.com/wp-content/uploads/GITR- 2014-Cisco-Chapter.pdf. Accessed on May 27th, 2015.

[3] Bringing Big Data to the Enterprise, IBM [Online]. Available: http://www-01.ibm.com/software/in/data/bigdata/. Accessed on May 27th, 2015.

[4] J. Gantz et al., "The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East," IDC IVIEW, Sponsored by EMC Corporation. Available at: http://www.emc.com /collateral /analyst-reports /idc-digital-universe-united-states. pdf. Accessed on May 27th, 2015.

[5] Tomorrow's Internet Today, CISCO [Online]. Available: http:// www.cisco.com/c/dam/en/us/products/collateral/routers/ asr-9000-series-aggregation-services-routers/brochure_tomorrows_ internet_today.pdf. Accessed on May 27th, 2015.

[6] R. Ranjan, "Streaming Big Data Processing in Datacentre Clouds, " IEEE Cloud Computing, BlueSkies Column, vol. 1, no. 1, pp. 78–83, May 2014.

[7] L. Wang and R. Ranjan, "Processing distributed internet of things data in clouds, " IEEE Cloud Computing, BlueSkies Column, vol. 2, no. 1, pp. 76–80, Apr. 2015.

SMART BANK GUARD SECURITY SYSTEM IMPLEMENTATION WITH THEFT IDENTIFICATION USING PATTERN ANALYZER

P. Sugapriya[#1], Mrs. K. Amsavalli[*2], Mr. K. Karnavel[*3], Ms. R. Elakiya[*4]

[#1] *PG Student, Dept. of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai*
[*2,*3,*4,] *Assistant Professor, Dept. of Computer Science and Engineering, Anand Institute of Higher Technology, Chennai*

p.sugapriya92@gmail.com

Abstract **– Security and Authentication of individuals is necessary for our daily lives especially in Bank lockers. But the security provided with bank systems has some back-doors. It has been improved by using techniques like pattern recognition comparing these existing traits, there is still need for considerable computer vision. Pattern recognition is a particular type of biometric system that can be used to reliably identify a person uniquely by analyzing the patterns found in OPEN CV image processing is used in this security system to authenticate user. In this system a new approach is provided for banking system. Initially pattern flow are collected as datasets and maintained in bank agent server. The machine has a camera to capture the pattern flow of user and sent for processing features of the logic were compared and user where recognized. In addition to the authentication of user there is another system to identify the user before that RFID tad checking is needed. Image processing is used and keypad password is needed for another level of security.**

Index Terms– **Introduction, Security, Smart Card, Authentication, Wireless Communication, Open CV, Password.**

I.INTRODUCTION

Banking is one of the sectors where technology and advancements in technologies have not been utilized to the fullest potential. Be in security system or access systems or even in material handling in banks. For example in the security systems even today very old practices are followed that can be made lot better using technologies like open CV which is easily usable and also easy to implement at a consumer level. In this present age, safety has becomes an essential issue for most of the people especially in the rural and urban areas. Some people will try to cheat or steal the property which may endanger the safety of money in the bank, house, and office. To overcome the security threat, a most of people will install bunch of locks or alarm system.

There are many types of alarm systems available in the market which utilizes different types of sensor. The sensor can detect different types of changes occur in the surrounding and the changes will be processed to be given out a alert according to the pre-set value. By the same time this system may not be good for all the time. In this paper we have implemented safety of the money in the bank locker, house, and office (treasury) by using RFID and GSM technology which will be more secure than other systems. Radio-frequency identification (RFID) based access-control system allows only authorized persons to open the bank locker with GSM technology. Basically, an RFID system consists of an antenna or coil, a transceiver (with decoder) and a transponder (RF tag) electronically programmed with unique information. There are many different types of RFID systems in the market. These are categorized on the basis of their frequency ranges. Some of the most commonly used RFID kits are low-frequency (30-500 kHz), mid-frequency (900 kHz-1500MHz) and high-frequency (2.4-2.5GHz)[1]. The passive tags are lighter and less expensive than the active tags. Global system for mobile communication (GSM) is a globally accepted standard.

Several GSM is a common European mobile telephone standard for a mobile cellular radio system operating at 900 MHz In the current work,SIM300 GSM module is used. The SIM300 module is a Tri-band GSM/GPRS solution in a compact plug in module featuring an industry-standard interface. It delivers voice, data and fax in a small form factor with low power consumption. In this paper we have designed and implemented a bank locker security system based on RFID and GSM technology. In this system only authentic person can be recovered money from bank locker with two password protection method.

Implementing sensors vibration, temperature sensor on the door side for security purpose and on machine side three level of authentication is needed .first one is RFID tag is provided for authentication of user id ,next camera is installed to capture the pattern password of user and with the help of image processing using OPEN CV to recognize the user pattern and the authentication for banking is provided and keypad password is need another level authentication for users access of banking is permitted for thief an immediate door lock is applied and intimate message to bank manager. This system is secure and less cost it will be a best banking system. Timer is on for accessing the bank locker it's locked automatically while the user exceeds the time as well as message notification also intimated to the manager.

II.MOTIVATION

The motivation of the proposal is to achieve the following:
More secure
Authentication only used
privacy management

III. LITERATURE SURVEY

1. Prabhakar and pankanti(1997) proposed Biometrics offers greater security and convenience than traditional methods of personal recognition. In some applications, biometrics can replace or supplement the existing technology.
2. Mary Lourde and Dushyant Khosla (2010) says Perhaps the most important application of accurate personal identification is securing limited access systems from malicious attacks. Among all the presently employed biometric techniques, fingerprint identification systems have received the most attention due to the long history of fingerprints and their extensive use in forensics. This paper deals with the issue of selection of an optimal algorithm for fingerprint matching in sorder to design a system that matches required specifications in performance and accuracy.
3. Gayathri and Selvakumari (2014) Access control system forms a vital link in a security chain. The Fingerprint and password based security system presented here is an access control system that allows only authorized persons to access a restricted area. We have implemented a locker security system based on fingerprint, password and GSM technology containing door locking system which can activate, authenticate and validate the user and unlock the door in real time for locker secure.
4. Arun Ross and salil prabhakar (2004) 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.
5. Kamble and Bharti (2012) the biometrics, fingerprint recognition is one of the most reliable and promising personal identification technologies. Fingerprints are the most widely used biometric feature for person identification and verification. But in this paper we proposed that fingerprint verification of ATM (Automatic Teller Machine) security system using the biometric with hybridization. The fingerprint trait is chosen, because of its availability, reliability and high accuracy.
6. Abhijeet Kaleand Sunpreet Kaur Nanda (2012) The GSM based communication helps the owner and concerned authorities to take necessary and timely action in order to prevent the theft. The LDR circuit is interfaced using a relay circuit with an Arduino microcontroller board. Efficacy of the proposed system can be seen in its immediate intimation regarding the incident. The proposed designed system is very effective and inexpensive.
7. Vanga Odelu, Ashok Kumar Das, and Adrijit Goswami (2008) new secure multiserver authentication protocol using biometric-based smart cardand ECC with more security functionalities. Using the Burrows-Abadi-Needham (BAN) logic, we show that our scheme providessecure authentication. In addition, we simulate our scheme for theformal security verification using the widely-accepted and usedAVISPA (Automated Validation of Internet Security Protocolsand Applications) tool, and show that our scheme is secure against passive and active attacks. Our scheme provides highsecurity along with low communication cost, computational cost,and variety of security features.
8. Joseph Lewis (2012) says that Biometric and GSM technology for bank lockers. Because in this system bank will collect the biometric data of each person for accessing the lockers because in this system only autheniticated person recover the money ,documents from the lockers. It is stored individual identity of a person and GSM is used for sending and receiving message.

IV. CONCLUSION OF LITERATURE SURVEY

A biometric system is essentially a pattern recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioral characteristic for identify a person. The behavioral characteristic include signature, gait, speech keystroke pattern, and gait these character are changer with age and environment .Physiological characteristic include fingerprint, face and iris etc. This character is remaining unchanged through life of person Biometric system operates as verification mode or identification mode depending upon on the requirement of application In verification mode, the system validates a person's identity by comparing the captured biometric characteristic with the individual's biometric template which is restored in the system data base.so the biometric is the essential tool for user identification in identify management system now we will discuss about some physical biometric parameter.Face recognition system is based on the idea that each human being is different and unique in creation. If we elucidate this, facial structure has parts that are unique to each person like fingerprint.

V.OPENCV

Open CV supports a wide variety of programming languages such as C++.Combining the best qualities of the Open CV C++ API and Python language. Opencv python is a library of python bindings designed to solve computer vision problems.python is general purpose programming language started by Guido van

Rossum that became very popular very quickly, mainly because of its simplicity and code readability.used to form.It enables the programmer to languages to express ideas in fewer lines of code without reducing readability.
Compared to languages like C/C++, Python is slower. That said, Python can be easily extended with C/C++, which allows us to write computationally intensive code in C/C++ and create python wrappers that can be used as python modules.
OpenCV-python makes use of NUMPY,which is a highly optimized library for numerical operations with a MATLAB-style syntax.All the openCV array structures are converted to and from Numpy arrays. This also makes it easier to integrate with other libraries that use Numpy such as SciPy and Matplotlib.

.

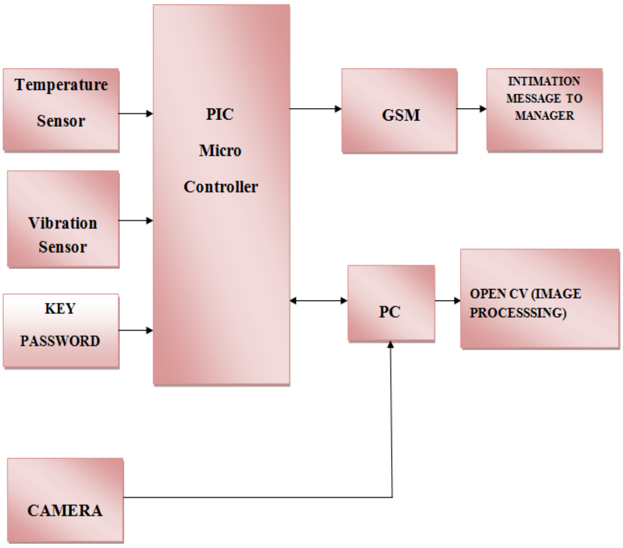


Fig1. Block Diagram of experimental arrangement

VI. SOFTWARE PROGRAM TESTING

The software program is written in EMBEDDED ‘C’ language and compiled by HI-TECH C compiler using MPLAB IDE software. The compiler is used to convert middle level language into machine level language. After compiler operation the hex code is generated and stored in the computer. The hex is nothing but machine level language understands by the micro controller. The hex code of the program is burnt into the ROM (Flash memory) of PIC16F877A by using PICKIT2 Programmer.

VI. MICROCONTROLLER

It is High performance RISC CPU machine. ONLY have 35 simple word instructions. Operating speed: clock input (200MHz), instruction cycle (200nS). Up to 368×8bit of RAM (data memory), 256×8 of EEPROM (data memory), 8k×14 of flash memory. Wide operating voltage range (2.0 – 5.56). volts.2 8 bit timer and one 16 bit timer is available10bit multi-channel A/D converter Synchronous Serial Port (ssp).with SPI (master code) and I2C (master/slave).100000 times erase/write cycle enhanced memory.1000000 times erase/write cycle data EEPROM memory.

VII. RFIDCARD

RFID" stands for Radio Frequency Identification. The tag's antenna picks up signals from an RFID reader or scanner and then returns the signal, usually with some additional data (like a unique serial number or other customized information). RFID system consists three components: an antenna or coil, a transceiver (with decoder) and a transponder (RF tag) electronically programmed with unique information. An RFID reader is a device that is used to interrogate an RFID tag. The reader has an antenna that emits radio waves; the tag responds by sending back its data.

VIII.GSM

The GSM modem is a specialized type of modem which accepts a SIM card operates on a subscriber’s mobile number over a network , just like a cellular phone .modem sim900 is a tri-band GSM/GPRS engine that works on EGSM900MHz, DCS1800MHz and PCS1900MHz frequencies. GSM Modem is RS232-logic level compatible. The signal at pin 11 of the microcontroller is sent to the GSM modem through pin 11 of max232.this signal is received at pin2(RX) of the GSM modem.The GSM modem transmits the signal from pin(TX) to the microcontroller through MAX232,which is received at pin 10 of IC1.

IX. SERIAL COMMUNICATION

Introduction The purpose of this application note is to attempt to describe the main elements in Serial Communication. This application note attempts to cover enough technical details of RS232, RS422 and RS485. 1.1. DCE and DTE Devices DTE stands for Data Terminal Equipment, and DCE stands for Data Communications Equipment. These terms are used to indicate the pin-out for the connectors on a device and the direction of the signals on the pins. Your computer is a DTE device, while most other devices such as modem and other serial devices are usually DCE devices. RS-232 has been around as a standard for decades as an electrical interface between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) such as modems or DSUs. It appears under different incarnations such as RS-232C, RS-232D, V.24, V.28 or V.10. RS-232 is used for asynchronous data transfer as well as synchronous links such as SDLC, HDLC, Frame Relay and X.25 1.2. Synchronous data transfer In program-to-program communication, synchronous communication requires that each end of an exchange of communication respond in turn without initiating a new communication.

A typical activity that might use a synchronous protocol would be a transmission of files from one point to another In this paper, we have first reviewed the recently proposed we are using locker key for banking though they are secured there are some disadvantages .It may be provide wrong person access the account. So in our project we are implementing sensors vibration, temperature sensor on the door side for security purpose and on machine side three level of authentication is needed .first one is RFID tag is provided for authentication of user id ,next camera is installed to capture the pattern password of user and with the help of image processing using OPEN CV to recognize the user pattern and the authentication for banking is provided and keypad password is need another level authentication for users access of banking is permitted for thief an immediate door lock is applied and intimate message to bank manager this system is secure and less cost it will be a best banking system. Timer is on for accessing the bank locker it's locked automatically while the user exceeds the time as well as message notification also intimated to the manager.

REFERENCES

[1] Prabhakar,s, pankanti s,and jain, A.K "Biometric recognition:Security and privacy concern:Security and Privacy,IEEE Volume:1 Issue:2.

[2] Mary Lourde R and Dushyant Khosla "Fingerprint Identification in Biometric Security Systems" International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010

[3] M.Gayathri, P.Selvakumari, R.Brindha "Fingerprint and GSM based Security System" International Journal of Engineering Sciences & Research Technology, ISSN: 2277-9655, Gayathri et al.3(4): April, 2014.

[4] Anil K. Jain, Arun Ross and salil prabhakar "An Introduction to Biometric Recognition"IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, no. 1, January 2004.

[5] D.Shekar and Goud and Ishaq Md and PJ.Saritha "A Secured Approach for Authentication System using Fingerprint and Iris" Global Journal of Advanced

2DOF PID CONTROLLER DESIGN FOR A NON LINEAR BIOREACTOR USING HEURISTIC ALGORITHM

M.Vishal#1, G. Hari Hara Sudhan*2, S. Vishal*3

Students, Department of EIE, St.Joseph's College of Engineering, Chennai 600 119

vishalnarasimhan18@gmail.com

hariharasudhang@rocketmail.com

vishaljosh1996@gmail.com

***Abstract*— In this paper, PID controller design is proposed for a bioreactor system using the Firefly Algorithm (FA). Objective function minimization is considered to monitor the FA towards the optimal controller solutions. In this work, ten trials are considered and the best value among the trial is chosen as the optimal solution. The performance of the proposed controller design procedure is validated using the heuristic methods, such as Genetic Algorithm (GA), Particle Swarm Optimization (PSO) and Bacterial Foraging Optimization (BFO) existing in the literature. The simulation result shows that, proposed FA based 2DOFPID offers better convergence, reference tracking, input disturbance rejection and load disturbance rejection performances compared with GA, PSO and BFO algorithms.**

Index Terms— *Bioreactor, 2DOFPID, Firefly algorithm, Convergence, Performance measure.*

I. INTRODUCTION

In recent years, many efforts have been attempted to design optimal and robust controllers for a class of chemical systems. Bioreactor is one of the important chemical system which plays a vital role in biochemical industry to produce very important chemical and medical products. During the closed loop operation, optimized controllers are very essential for this process in order to minimize the waste and to maximize the production rate.

In the control literature, evolutionary algorithm based optimization is emerged as a powerful tool for finding the solutions for a variety of control engineering applications. Soft computing based PID controller parameter optimization is widely addressed by the researchers [1-5]. Recently, Rajinikanth and Latha [6-10], Latha et al. [3] and Ramya and Latha [11] have attempted evolutionary algorithm based PID and modified forms of PID tuning for a class of stable and unstable process models. In their work, error minimization (ISE and IAE) is highly prioritized as a performance measure and it monitors the algorithm based controller tuning, until the controller values converge to an optimised value.

In this work, heuristic algorithm based PID controller with prefilter (FPID) [9] and Setpoint Weighted PID (SWPID) [10] controller design process is proposed for a nonlinear bioreactor model existing in the literature [13-15]. A comparative study also carriedout with heuristic algorithms, such as FA, GA, PSO and BFO methods existing in the literature.

II. PROCESS DESCRIPTION

Bioreactor is an important unit in biochemical process plants used to produce significant chemical and biochemical products. In this unit, living microbes are converted into biochemical products such as beverages, antibiotics, vaccines and industrial solvents [14]. The excellence of the final product of a bioreactor relies on the control loop which monitors the microbial growth based on setpoint. Therefore, in recent years, a number of controller design methods are proposed for the bench mark bioreactor model [4-11].

In literature, a number of studies are available for model based control of bioreactor. The following mathematical equations considered in this research work, can describe a variety of industrial bioreactors [13-15]:

Cell balance : $\frac{dX}{dt} = (\mu - D)X$ (1)

Substrate balance : $\frac{dS}{dt} = D(S_f - S) - \frac{\mu X}{Y}$ (2)

Product balance: $\frac{dP}{dt} = -D\ P + (\alpha\ \mu + \beta)\ X$ (3)

Monod kinetics: $\mu = \frac{\mu_{max}\ S}{K_m + S}$ (4)

where, 'μ' is the specific growth rate, 'X' the biomass concentration, 'S' the substrate concentration and 'α' and 'β' are yield parameters for the product. At steady state, the variables will be; X = Xs, S = Ss, and P = Ps.
The transfer function of the stable bioreactor model considered in this study is given below:

$$G(s) = \frac{-1.53\,s - 0.4588}{s^2 + 2.564\,s + 0.6792}\,e^{-0.25\,s} \qquad (5)$$

III. CONTROLLER STRUCTURE

To achieve a satisfactory reference tracking and disturbance rejection operation, the controller should have

optimal values of K_p, K_i and K_d. In this study, parallel PID controller is considered to achieve the preferred response.
The parallel PID structure is given below:

$$G_C(s) = K_p\, e(t) + K_i \int_0^T e(t)\, dt + K_d \frac{de(t)}{dt} \qquad (6)$$

$$G_{PID}(s) = K_p \left[1 + \frac{1}{T_i\, s} + T_d\, s \right] \qquad (7)$$

where $K_p / T_i = K_i$ and $K_p{*}T_d = K_d$.

In the proposed work, the following Objective Function (OF) is considered:
$J_{min}(PID) = (w_1.IAE) + (w_2.ISE) + (w_3.M_p)$ (8)
where w_1=w_2= 10 and w_3=5, IAE = Integral Absolute Error, ISE = Integral Square Error and M_p = Peak overshoot.
The following Two Degree Of Freedom (2DOF) PID structure is considered to control the bioreactor process model.
Fig.1 depicts the PID controller with prefilter structure (FPID). In this structure, the total number of controller parameters to be tuned are four, such as K_p, K_i, K_d and T_f . In this, a first order filter '1/(T_fs+1)' is pleased between the setpoint and the error detector [9].

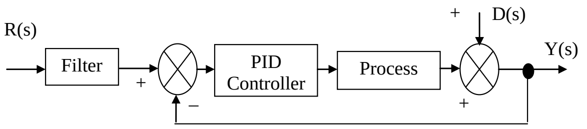


Fig.2 depicts the setpoint weighted PID controller (SWPID). In this structure, the total number of controller parameters to be tuned are five, such as K_p, K_i, K_d, α and β.

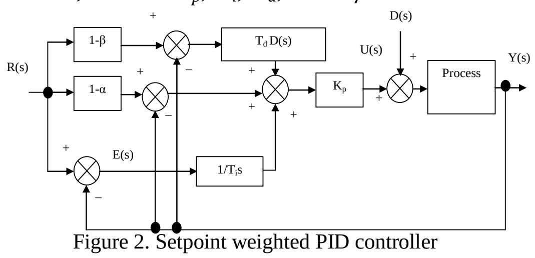


Figure 2. Setpoint weighted PID controller

$$PID_1 = K_p(1-\alpha) + \frac{K_i}{s} + (1-\beta)K_d \qquad (9)$$

$$PID_2 = K_p * \alpha + K_d * \beta \qquad (10)$$

Eqn. (9) and (10) depicts the controller values of the setpoint weighted PID. Generally it is a PID-PD structure with a setpoint weighting parameters [10,16].

IV. HEURISTIC ALGORITHMS

In recent years, heuristic algorithm based PID controller design is widely addressed by most of the researchers. In this work, the Firefly Algorithm (FA) based controller design is adopted to design the 2DOF PID controller for the bioreactor process. The detailed description of the FA algorithm based controller design procedure for bioreactor process can be found in [5,12].

In order to evaluate the performance of the proposed FA based procedure, a simulation study is carried with heuristic methods such as Genetic Algorithm (GA), Particle Swarm Optimization (PSO) and Bacterial Foraging Optimization (BFO) existing in the literature. To perform a fair comparison, similar computational effort such as the maximum generation size (G_{max} = 300), population size (20), search dimension (4 for FPID and 5 for SWPID), and number of trials are chosen as ten.

Other heuristic algorithms considered in this study are given below:

- GA is a most successful evolutionary method, extensively adapted for engineering optimization problem. In the GA based search, the following parameters are assigned: crossover probability is selected as 0.5, and mutation probability is set as 0.25. Roulette wheel based selection criterion is considered in this study [1,2].
- PSO algorithm is commonly used by the researchers to solve complex optimization problems. In this work, the PSO algorithm considered in the literature is chosen [3]. The following PSO parameters are considered: Number of bird step is considered as 20; the cognitive (C_1) and global (C_2) search parameter is assigned the value of 2.
- The BFO algorithm always provides stable convergence and better result compared with other methods. In this work, BFO algorithm discussed by Rajinikanth and Latha is adopted [8-10].

During the controller design process, the heuristic algorithm continuously explores the search space until the objective function is minimized. In this work, a four dimensional search is considered for the FPID and a five dimensional search is considered for SWPID.

V. RESULTS AND DISCUSSIONS

This section presents the simulation result for the proposed controllers for the nonlinear bioreactor model. In this simulation study, the simulation time is assigned as 100 sec and a load disturbance of 0.5 (50% of setpoint value) is applied at 50 sec to evaluate the disturbance rejection performance of FPID and SWPID. In this simulation study, the controller design procedure is repeated ten times with each algorithm and the mean of the controller values are chosen as the optimized controller parameters. During the FPID design process, the dimension of search is chosen as four and for SWPID the dimension of search is chosen as five.

Initially the FA based FPID design is proposed for the bioreactor model (Eqn.5). Ten trials are performed on the model with the FA and the mean of the controller values, such as K_p, K_i, K_d and T_f are chosen as the optimal values. Similar procedure is repeated with GA, PSO and BFO algorithms and the obtained controller values are presented in Table 2. In order to assess the performance of the controller for reference tracking operation and the disturbance rejection operation, a unity step reference signal and a load disturbance of 0.5 is applied for the system and the error values, such as ISE and IAE are recorded as depicted in Table 1. Fig. 3 (a) and (b) shows the process response and controller response for the bioreactor model with FPID controller. From these results, it can be observed that, the FPID offers smooth reference tracking and smooth controller performance for the considered process model for servo and regulatory operations.

Later, the controller design procedure is implemented using the SWPID structure. Like the FPID, the controller design procedure is repeated ten times with FA, GA, PSO and BFO and the average values of K_p, K_i, $K_{d,}$ α, and β are recorded as in Table 2. Fig . 4 (a) and (b) depicts the process response and the controller output with the SWPID for the reference tracking and disturbance rejection operations. From Table 3, it can be observed that, the ISE and IAE values offered by FA is better than GA, PSO and BFO.

Table 1. FPID controller values and the corresponding ISE and IAE

Method	K_p	K_i	K_d	T_f	ISE	IAE
FA	- 0.6493	- 0.8814	- 0.2932	0.2973	0.899	2.519
GA	- 0.5718	- 0.7988	- 0.2004	0.4756	0.908	2.780
PSO	- 0.6911	- 0.7942	- 0.1878	0.5104	0.854	2.796
BFO	- 0.7047	- 0.7326	- 0.1094	0.4972	0.916	3.031

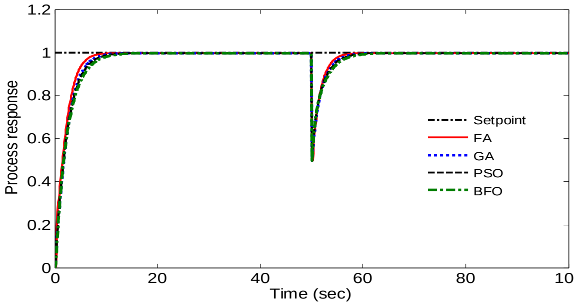


Figure 3. (a) Process response with FPID controller

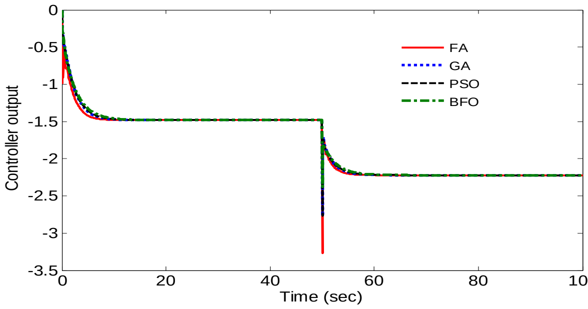


Figure 3. (b) Controller output with the FPID controller

Table 2. SWPID controller values and the corresponding ISE and IAE

Method	K_p	K_i	K_d	α	β	ISE
FA	*- 0.7103*	*- 0.6128*	*- 0.1936*	*0.5924*	*0.3987*	1.919
GA	- 0.6194	- 0.5103	- 0.2153	0.4982	0.1936	2.137
PSO	- 0.5284	- 0.3775	- 0.2087	0.2768	0.4173	2.506
BFO	- 0.5478	- 0.4772	- 0.2835	0.5187	0.4924	2.311

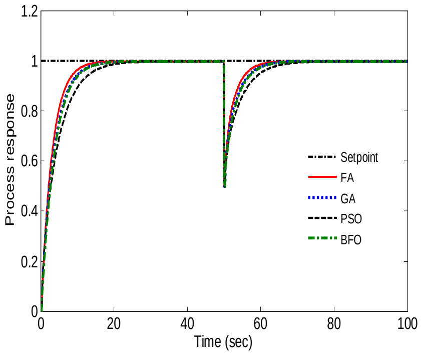


Figure 4. (a) Process response with SWPID controller

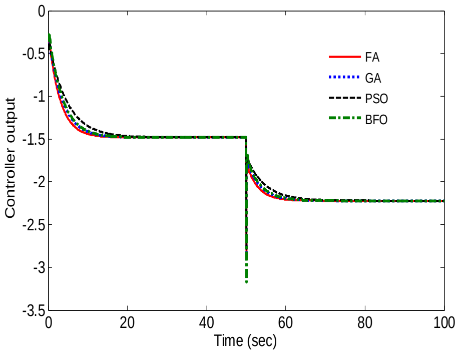
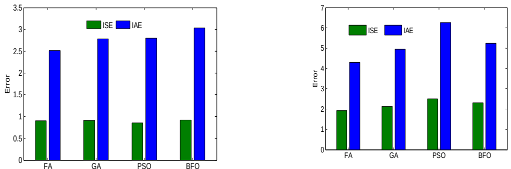


Figure 4. (b) Controller output with the SWPID controller



(a) FPID (b) SWPID

Figure 5. ISE and IAE values for the 2DOFPID controllers

Fig. 5 graphically represents the ISE and IAE values obtained with FPID and SWPID with FA, GA, PSO and PSO. From this, it is noted that the FA based algorithm offers enhanced result GA, PSO and BFO with a small ISE and IAE values

VI. CONCLUSIONS

In this paper, FA based FPID and SWPID controller design is proposed for bioreactor model and its reference tracking and disturbance rejection operation validated with GA, PSO and BFO algorithms existing in the literature. From this study, it is confirmed that, the FA tuned 2DOF PID offers better result than other heuristic algorithm tuned 2DOF PID. The FA based controller offers lesser ISE and IAE values for reference tracking and disturbance rejection operations compared with GA, PSO and BFO algorithm tuned controllers.

REFERENCES

[1] G. Sivagurunathan, and K. Saravanan, "Evolutionary Algorithms based Controller Optimization for a Real Time Spherical Tank System," Australian Journal of Basic and Applied Sciences, vol.8, no.3, pp.244-254, 2014.

[2] Iraj Hassanzadeh, and Saleh Mobayen, "Controller Design for Rotary Inverted Pendulum System Using Evolutionary Algorithms," Mathematical Problems in Engineering, vol. 2011, Article ID 572424, 17 pages, 2011. doi:10.1155/2011/572424

[3] K. Latha, V. Rajinikanth, and P. M. Surekha, "PSO-Based PID Controller Design for a Class of Stable and Unstable Systems," ISRN Artificial Intelligence, vol. 2013, Article ID 543607, 11 pages, 2013.

[4] N.S.M. Raja, and V. Rajinikanth, "Brownian Distribution Guided Bacterial Foraging Algorithm for Controller Design Problem," In: ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India- Vol I, (Eds: S.C. Satapathy et al.) Springer, AISC 248, pp. 141-148, 2014.

5. N.S.M. Raja, K.Suresh Manic, and V. Rajinikanth, "Firefly Algorithm with Various Randomization Parameters:An Analysis," In B.K. Panigrahi et al. (Eds.): SEMCCO 2013, Part.1, Lecture notes in computer science (LNCS 8297), pp. 110–121, 2013.

[5] V. Rajinikanth and K. Latha, "Identification and control of unstable biochemical reactor," International Journal of Chemical Engineering and Applications, vol. 1, no. 1, pp. 106–111, 2010.

[6] V. Rajinikanth and K. Latha, "Optimization of PID controller parameters for unstable chemical systems using soft computing technique," International Review of Chemical Engineering, vol. 3, no. 3, pp. 350–358, 2011.

[7] V. Rajinikanth, and K. Latha, "Controller Parameter Optimization for Nonlinear Systems Using Enhanced Bacteria Foraging Algorithm," Applied Computational Intelligence and Soft Computing, vol. 2012, Article ID 214264, 12 pages, 2012. doi:10.1155/2012/214264.

[8] V. Rajinikanth, and K. Latha, "Internal model control-proportional integral derivative controller tuning for first order plus time delayed unstable systems using bacterial foraging algorithm," Scientific Research and Essays, vol.7, no.40, pp. 3406-3420, 2012.

[9] V. Rajinikanth, and K.Latha, "Setpoint weighted PID controller tuning for unstable system using heuristic algorithm," Archives of Control Sciences, vol.22, no.4, 481-505, 2012.

[10] S. Ramya, and K. Latha, "Hybrid heuristic algorithm based controller tuning for a bioreactor," In proceedings of International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE), pp. 1 – 7, 2014. doi: 10.1109/ICGCCEE.2014.6922325.

[11] N.S.M. Raja, V. Rajinikanth, and K. Latha, "Otsu Based Optimal Multilevel Image Thresholding Using Firefly Algorithm," Modelling and Simulation in Engineering, vol. 2014, Article ID 794574, 17 pages, 2014.

[12] R. Padma Sree, and M. Chidambaram, "Control of Unstable Systems," Narosa Publishing House, New Delhi, India, 2006.

[13] A. K. Jana, "Chemical Process Modeling and Computer Simulation," Prentice-Hall, New Delhi, India, 2008.

[14] B. Wayne Bequette, "Process Control: Modeling, Design and Simulation," Prentice Hall, 2003.

[15] C. Chen, H. Hsia-Ping, and L. Horng-Jang, "Set-Point Weighted PID Controller Tuning for Time-Delayed Unstable Processes," Ind. Eng. Chem. Res., vol. 47, no.18, pp.6983-6990, 2008.

EDGE COMPUTING AND ITS APPLICATIONS

S.Umadevi[#1], yashodei[*2] and S.Kiruhika[*3]

[#1]Assistant professor,Department of CSE, IFET College of Engineering, Villupuram.
[*2]Assistant professor,Department of CSE, IFET College of Engineering, Villupuram.
[*3]B.E.Computer Science & Engineering, III year, IFET College of Engineering, Villupuram.

mamahima@gmail.com
skiruthika55@gmail.com

Abstract—**Fog Computing is also said to be as a edge computing and it is a paradigm that extends Cloud computing and services to the edge of the network. Similar to Cloud, Fog provides data, compute, storage, and application services to end-users. In this article, we elaborate the motivation and advantages of Fog computing, and analyze its applications in a series of real scenarios, such as Smart Grid, smart traffic lights in vehicular networks and software defined networks. Security and privacy issues are further disclosed according to current Fog computing paradigm. As an example, we study a typical attack, man-in-the-middle attack, for the discussion of security in Fog computing. We investigate the stealthy features of this attack by examining its CPU and memory consumption on Fog device.**

***Index Terms*—Fog Computing, Cloud Computing, Internet of Things, Software Defined Networks.**

I. INTRODUCTION

CISCO recently delivered the vision of fog computing to enable applications on billions of connected devices, already connected in the Internet of Things (IoT), to run directly at the network edge [1]. Customers can develop, manage and run software applications on Cisco I Ox framework of networked devices, including hardened routers, switches and IP video cameras. Cisco I Ox brings the open source Linux and Cisco IOS network operating system together in a single networked device (initially in routers). The open application environment encourages more developers to bring their own applications and connectivity interfaces at the edge of the network. Regardless of Cisco's practices, we first answer the questions of what the Fog computing is and what are the differences between Fog and Cloud. Both Cloud and Fog provide data, computation, storage and application services to end-users. We adopt a simple three level hierarchy as in Figure 1. In this framework, each smart thing is attached to one of Fog devices. Fog devices could be interconnected and each of them is linked to the Cloud.In this article, we take a close look at the Fog computing paradigm. The goal of this research is to investigate Fog computing advantages for services in several domains, such as Smart Grid, wireless sensor networks, Internet of Things (IoT) and software defined networks (SDNs). We examine the state-of-the-art and disclose some general issues in Fog computing including security, privacy, trust, and service migration among Fog devices and between Fog and Cloud. We finally conclude this article with discussion of future work

II. WHY DO WE NEED FOG?

In the past few years, Cloud computing has provided many opportunities for enterprises by offering their customers a range of computing services. Current "pay-as-you-go" Cloud computing model becomes an efficient alternative to owning and managing private data centers for customers facing Web applications and batch processing [3] Cloud computing frees the enterprises and their end users from the specification of many details, such as storage resources, computation limitation and network communication cost. However, this bliss becomesa problem for latency-sensitive applications, which require nodes in the vicinity to meet their delay requirements [2]. When techniques and devices of IoT are getting more involved in people's life, current Cloud computing paradigm can hardly satisfy their requirements of mobility support, location aware-ness and low latency.

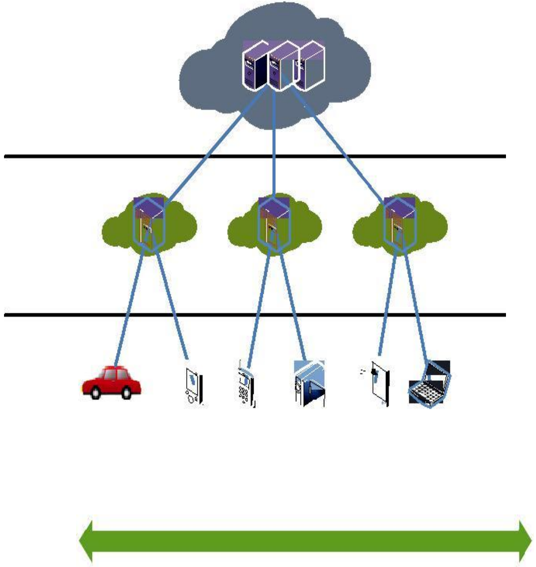


Fig. 1.Fog between edge and cloud.

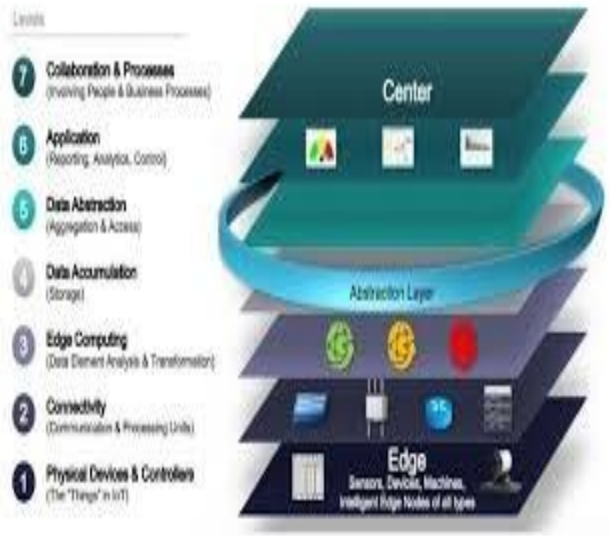

Levels
7 Collaboration & Processes
(Involving People & Business Processes)
6 Application
(Reporting, Analytics, Control)
5 Data Abstraction
(Aggregation & Access)
4 Data Accumulation
(Storage)
3 Edge Computing
(Data Element Analysis & Transformation)
2 Connectivity
(Communication & Processing Units)
1 Physical Devices & Controllers
(The "Things" in IoT)
Center
Abstraction Layer
Edge
Sensors, Devices, Machines,
Intelligent Edge Nodes of all types

Fig.2.Fog layer in computing

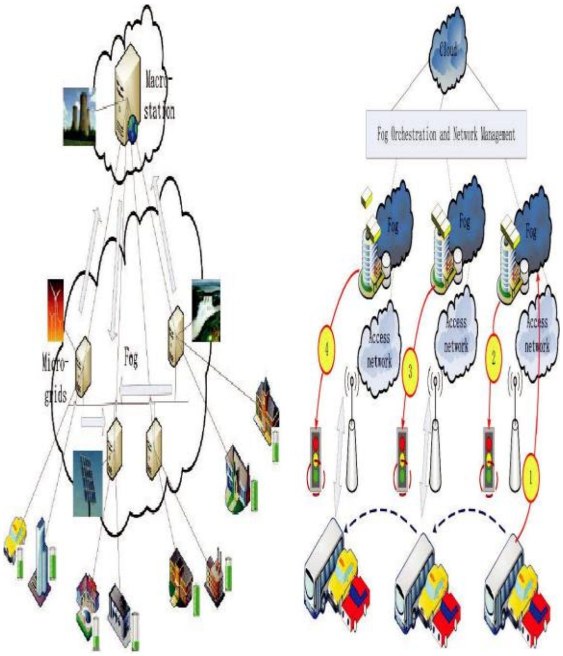


Fig. 3. Fog computing in smart grid. Fig. 4. Fog computing in smart traffic lights and connected vehicles

III. WHAT CAN WE DO WITH FOG?

We elaborate on the role of Fog computing in the following six motivating scenarios. The advantages of Fog computing satisfy the requirements of applications in these scenarios.

Smart Grid: Energy load balancing applications may run on network edge devices, such as smart meters and micro-grids [4]. Based on energy demand, availability and the lowest price, these devices automatically switch to alternative energies like solar and wind. As shown in Figure 2, Fog collectors at the edge process the data generated by grid sensors and devices, and issue control commands to the actuators [2]. They also filter the data to be consumed locally, and send the rest to the higher tiers for visualization, real-time reports and transactional analytics. Fog supports ephemeral storage at the lowest tier to semi-permanent storage at the highest tier. Global coverage is provided by the Cloud with business intelligence analytics.

Smart Traffic Lights and Connected Vehicles: Video camera that senses an ambulance flashing lights can automatically change street lights to open lanes for the vehicle to pass through traffic. Smart street lights interact locally with sensors and detect presence of pedestrian and bikers, and measure the distance and speed of approaching vehicles. As shown in Figure 3, intelligent lighting turns on once a sensor identifies movement and switches off as traffic passes. Neighboring smart lights serving as Fog devices coordinate to create green traffic wave and send warning signals to approaching vehicles [2].

Wireless access points like Wi-Fi, 3G, road-side units and smart traffic lights are deployed along the roads. Vehicles-to-Vehicle, vehicle to access points, and access points to access points interactions enrich the application of this scenario.

Wireless Sensor and Actuator Networks: Traditional wire-less sensor networks fall short in applications that go beyond sensing and tracking, but require actuators to exert physical actions like opening, closing or even carrying sensors [2].

Decentralized Smart Building Control: The applications of this scenario are facilitated by wireless sensors deployed to measure temperature, humidity, or levels of various gases in the building atmosphere. In this case, information can be exchanged among all sensors in a floor, and their readings can be combined to form reliable measurements. Sensors will use distributed decision making and activation at Fog devices to react to data.

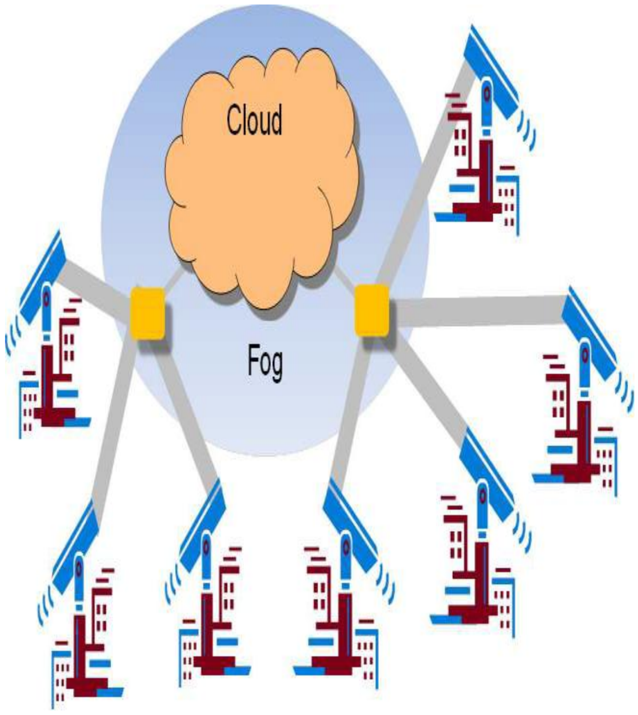


Fig.4.Represents the formation of cloud to fog computing

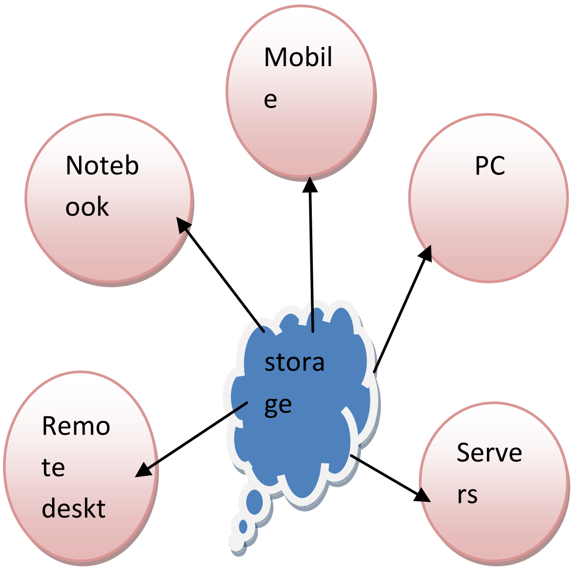


Fig.5.storage area in Fig

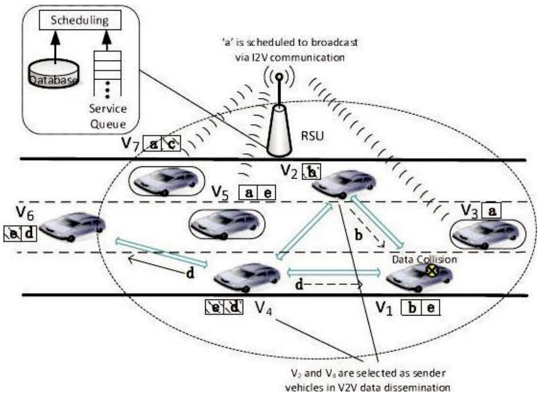


Fig. 6.Fog computing in SDN in vehicular networks [6].

The system components may then work together to lower the temperature, inject fresh air or open windows. Air conditioners can remove moisture from the air or increase the humidity. Sensors can also trace and react to movements (e.g, by turning light on or off). Fog devices could be assigned at each floor and could collaborate on higher level of actuation. With Fog computing applied in this scenario, smart buildings can maintain their fabric, external and internal environments to conserve energy, water and other resources.

IoT and Cyber-physical systems (CPSs): Fog computing based systems are becoming an important class of IoT and CPSs. Based on the traditional information carriers including Internet and telecommunication network, IoT is a network that can interconnect ordinary physical objects with identified addresses [5]. CPSs feature a tight combination of the system's computational and physical elements. CPSs also coordinate the integration of computer and information centric physical and engineered systems. IoT and CPSs promise to transform our world with new relationships between computer-based control and communication systems, engineered systems and physical reality. Fog computing in this scenario is built on the concepts of embedded systems in which software programs and computers are embedded in devices for reasons other than computation alone.

Software Defined Networks (SDN): As shown in Figure 6, Fog computing framework can be applied to implement the SDN concept for vehicular networks. SDN is an emergent computing and networking paradigm, and became one of the most popular topics in IT industry [7]. It separates control and data communication layers. Control is done at a centralized server, and nodes follow communication path decided by the server. The centralized server may need distributed implementation. SDN concept was studied in WLAN, wireless sensor and mesh networks, but they do not involve multi-hop wireless communication, multi-hop routing.

Smart Parking Deployment :
□ Parking Sensors are deployed on the curb in all the streets of the pilot area (reliability of car detection is over 97%) . Parking spaces are marked with numbers.Multi-Services kiosks are deployed on the streets.

Fig.7.represents the smart parking in mobile apps

Smart Mobility: EzPark:

□ Real-time info about parking availability. Real-time and Predictive Traffic** information including itinerary calculation . Real-time info about parking pricing . Pay ByPhone/NFC payment Impact . Parking commuters benefit from time saving for a search and easier way to manage overall transportation means .Smart Parking leads to about 30% net increase revenues for the city .Parking maintenance drops by 5% .Mobility optimization reduce traffic congestion up to 30%

EzMove*:*

□ Real-time Information about public and electric car sharing service (itinerary calculation) . Booking service for electric car sharing .NFC Payment for electric car sharing

EzCity :

□ On going creation of e-Service to inform users (managed by the City) .Retailer couponing and deals**

Street Light Management :

□ Lamp intensity monitored according to information sent by luminosity & traffic sensors. Diverse sensors taking into account multiple criteria: natural light (day or night), weather conditions (eg: more light in the event of fog), presence of cars (Light substitute with car headlight), presence of physical persons (less light in case of higher concentration of persons and more light in the event of an isolated person) .Match comfort and security dimensions .

Street Lighting Evolution :

□ Beyond smart LED, city leaders and street lighting vendor are envisioning street light as a multi service platform . Street lights are everywhere and once connected to power and network they could host many services: sensors, wireless transceiver (wifi, PAN, small cell), digital signs, communication . Philips (e.g. Barcelona) and others are leading the initiative .However average lifespan of street light pole is 30 to 40 years. Replacing all light pole with next-generation street light is a long term process.

Fig.8.represents smart lighting

The fog computing environment which represents the smart applications on itself. In which the cities has based on their smart applications towards on its new technology.

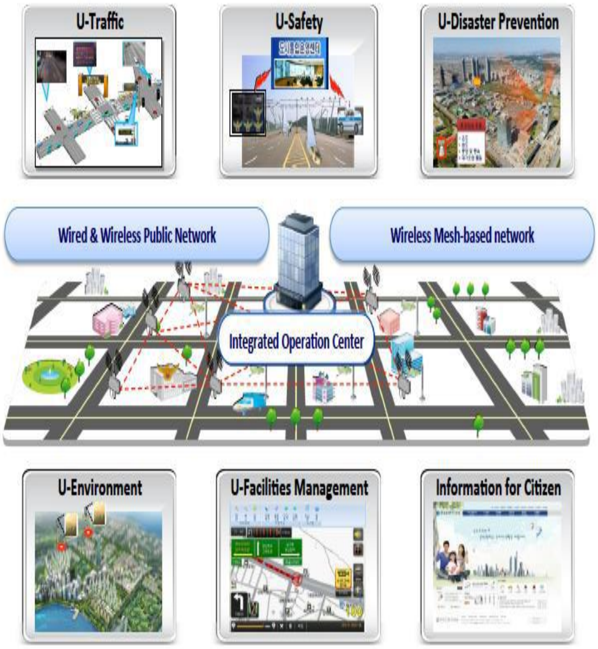


Fig.9.smart city

IV.RELATED WORK

K. Hong et al. proposed mobile Fog in [1]. This is a high level programming model for geo-spatially distributed, large-scale and latency-sensitive future Internet applications. Following the logical structure shown in Figure 1, low-latency processing occurs near the edge while latency-tolerant large-scope aggregation is performed on powerful resources in the core of the network (normally the Cloud). Mobile Fog consists of a set of event handlers and functions that an application can call. Mobile Fog model is not presented as generic model, but is built for particular application, while leaving out functions that deal with technical challenges of involved image processing primitives. Fog computing approach reduces latency and network traffic.

B. Ottenwalder et al. presented a placement and migration method for Cloud and Fog resources providers [3]. It ensures application-defined end-to-end latency restrictions and reduces the network utilization by planning the migration ahead of time. They also show how the application knowledge of the complex event processing system can be used to reduce the required bandwidth of virtual machines during their migration. Network intensive operators are placed on distributed Fog devices while computationally intensive operators are in the Cloud. Migration costs are amortized by selecting migration targets that ensure a low expected network utilization for a sufficiently long time.

B. Similar Work

BETaaS [1] proposed replacing Cloud as the residen-t for machine-to-machine applications by ‘local Cloud’ of gateways. The ‘local Cloud’ is composed of devices that provide smart things with connectivity to the Internet, such as smart phones, home routers and road-side units. This enables applications that are limited in time and space to require simple and repetitive interactions. It also enables the applications to respond in consistent manner.

Demand Response Management (DRM) is a key component in the smart grid to effectively reduce power generation costs and user bills. The work [6] addressed the DRM problem in a network of multiple utility companies and consumers where every entity is concerned about maximizing its own benefit. In their model, utility companies communicate witheach other, while users receive price information from utility companies and transmit their demand to them. They propose a Stackelberg game [7] between utility companies and end-users to maximize the revenue of each utility company and the payoff of each user. Stackelberg equilibrium of the game has a unique solution. They develop a distributed algorithm which converges to the equilibrium with only local information available for both utility companies and end-users. Utility companies play a non-cooperative game. They inform users whenever they change price, and users then update their demand vectors and inform utility companies. This iterates until convergence.
The main drawback of this algorithm is a significant communication overhead between users and utility companies. Though DRM helps to facilitate the reliability of power supply, the smart grid can be susceptible to privacy and security issues because of communication links between the utility companies and the consumers. They study the impact of an attacker who can manipulate the price information from the utility companies, and propose a scheme based on the concept of shared reserve power to improve the grid reliability and ensure its dependability.

The work [8] investigated how energy consumption may be optimized by taking into consideration the interaction between both parties. The energy price model is a function of total energy consumption. The objective function optimizes the difference between the value and cost of energy. The power supplier pulls consumers in a round-robin fashion, and provides them with energy price parameter and current consumption summary vector. Each user then optimizes his own schedule and reports it to the supplier, which in turn updates its energy price parameter before pulling the next consumers. This interaction between the power company and its consumers is modelled through a two-step centralized game, based on which the work [8] proposed the Game-Theoretic Energy Schedule (GTES) method. The objective of the GTES method is to reduce the peak to average power ratio by optimizing the users energy schedules.

The closest work for SDN in vehicular networks are several implementations in wireless sensor network and mesh networks . Moreover, B. Zhou et al. studied adaptive traffic light control for smoothing vehicles’ travel and maxi-mixing the traffic throughout for both single and multiple lanes [2]. In addition, the work [3] proposed a three-tier structure for traffic light control. First, an electronic toll collection (ETC) system is employed for collecting road traffic flow data and calculating the recommended speed. Second, radio antennas are installed near the traffic lights. Third, road traffic flow information can be obtained by wireless communication between the antennas and ETC devices. A branch-and-bound-based real-time traffic light control algorithm is designed to smooth vehicles’ travels.

V. SECURITY AND PRIVACY IN FOG COMPUTING

Security and privacy issues were not studied in the context of fog computing. They were studied in the context of s-mart grids [24] and machine-to-machine communications [25].

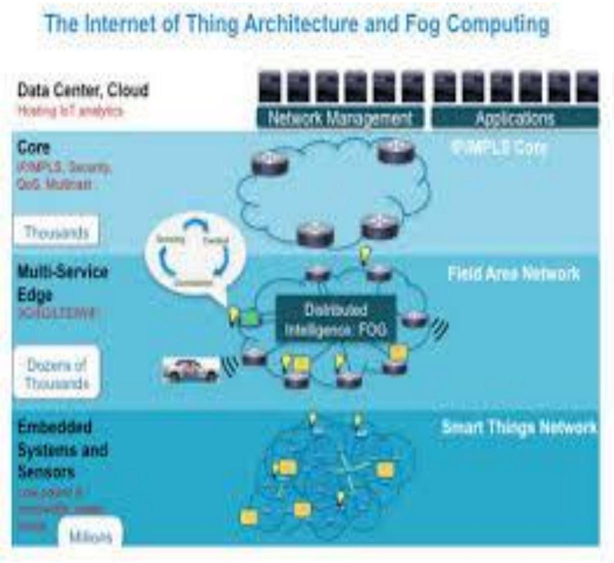


Fig.11.Thw internet of Things Architecture and Fog computing

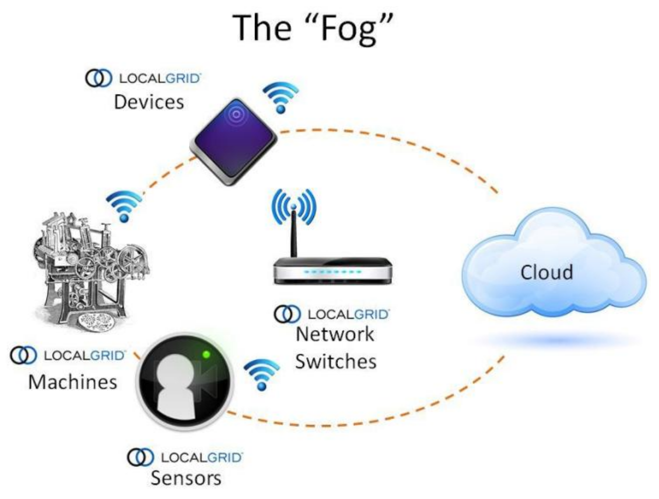


Fig.10.The Fog on IOT

There are security solutions for Cloud computing. However, they may not suit for Fog computing because Fog devices work at the edge of networks. The working surroundings of Fog devices will face with many threats which do not exist in well managed Cloud. In this section, we discuss the security and privacy issues in Fog Computing.

A. Security Issues

The main security issues are authentication at different levels of gateways as well as (in case of smart grids) at the smart meters installed in the consumer's home. Each smart meter and smart appliance has an IP address. A malicious user can either tamper with its own smart meter, report false readings, or spoof IP addresses. There are some solutions for the authentication problem. The work [6] elaborated public key infrastructure (PKI) based solutions which involve multicast authentication. Some authentication techniques using Diffie-Hellman key exchange have been discussed in [7]. Smart meters encrypt the data and send to the Fog device, such as a home-area network (HAN) gateway. HAN then decrypts the data, aggregates the results and then passes them forward.

Intrusion detection techniques can also be applied in Fog computing [8]. Intrusion in smart grids can be detected using either a signature-based method in which the patterns of behaviour are observed and checked against an already existing database of possible misbehaviors. Intrusion can also be captured by using an anomaly-based method in which an observed behaviour is compared with expected behaviour to check if there is a deviation. The work [9] develops an algorithm that monitors power flow results and detects anomalies in the input values that could have been modified by attacks. The algorithm detects intrusion by using principal component analysis to separate power flow variability into regular and irregular subspaces.

B. An Example: Man-in-the-Middle Attack

Man-in-the-middle attack has potential to become a typical attack in Fog computing. In this subsection, we take man-in-the-middle attack as an example to expose the security problems in Fog computing. In this attack, gateways serving as Fog devices may be compromised or replaced by fake ones [30]. Examples are KFC or Star Bar customers connecting to malicious access points which provide deceptive SSID as public legitimate ones

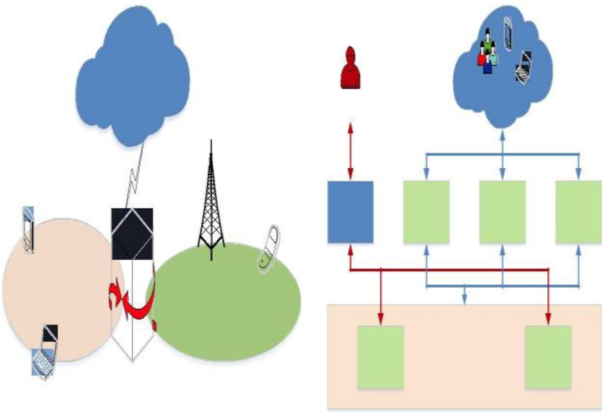


Fig. 12. A scenario for a man-in-the-middle attack towards Fog.

1) Environment Settings of Stealth Test: Man-in-the-middleattack can be very stealthy in Fog computing paradigm. This type of attack will consume only a small amount of resources in Fog devices, such as negligible CPU utilization and memory consumption. Therefore, traditional anomaly detection methods can hardly expose man-in-the-middle attack without noticeable features of this attack collected from the Fog. In order to examine how stealthy the man-in-the-middle attack can be, we implement an attack environment shown in Figure 5. In this scenario, a 3G user sends a video call to a WLAN user. Since the man-in-the-middle attack requires to control the communication between the 3G user and the WLAN user, the key of this attack is to compromise the gateway which serves as the Fog device.

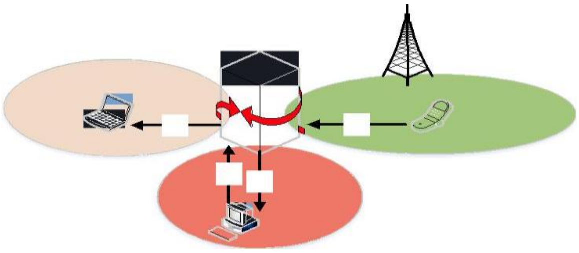
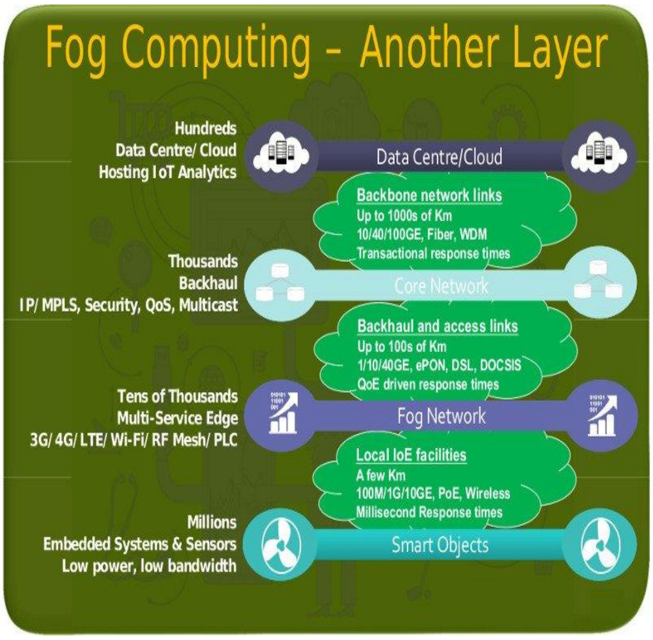


Fig. 13. The hijacked communication in Fog (e.g. from phone the environment.

Two steps are needed to realize the man-in-the-middle attack for the stealth test. First, we need to compromise the gateway, and second, we insert malicious code into the compromised system. For susceptible gateways, we can either refresh the ROM of a normal gateway or place a fake active point in Both methods can be easily implemented in the real world, such as in the KFC or Star Bar environments. In our experiment, we choose the former and use Broadcom BCM5354 as the gateway [31]. This device has a high-performance MIPS32 processor, IEEE 802.11 b/g MAC/PHY and USB2.0 controller. Video communication is set up on BCM5354 between a 3G mobile phone and a laptop which adopts Wi-Fi for connection. We refresh the ROM of BCM4354 and update its system to the open-source Linux kernel 2.4.

2) Work Flow of Man-in-the-Middle Attack:

The communication between 3G and WLAN needs a gateway to translate the data of different protocols into the suitable formats. Therefore, all the communication data will firstly arrive at the gateway and then be forwarded to other receivers. In our experiment, the man-in-the-middle attack is divided into four steps. We illustrate the hijacked communication from 3G to WLAN in Figure 7. In the first two steps, the embedded hook process of the gateway redirects the data received from the 3G user to the attacker. The attacker replays or modifies the data of the communication at his or her own computer, and then send the data back to the gateway. In the final step, the gateway forwards the data from the attacker to the WLAN user. In fact, the communication from the WLAN user will also be redirected to the attacker at first, and then be forwarded by the hook in the gateway to the 3G user.


Fog Computing - Another Layer

Hundreds
Data Centre/ Cloud
Hosting I oT Analytics

Data Centre/Cloud

Backbone network links
Up to 1000s of Km
10/40/100GE, Fiber, WDM
Transactional response times

Thousands
Backhaul
I P/ MPLS, Security, QoS, Multicast

Core Network

Backhaul and access links
Up to 100s of Km
1/10/40GE, ePON, DSL, DOCSIS
QoE driven response times

Tens of Thousands
Multi-Service Edge
3G/ 4G/ LTE/ Wi-Fi/ RF Mesh/ PLC

Fog Network

Local IoE facilities
A few Km
100M/1G/10GE, PoE, Wireless
Millisecond Response times

Millions
Embedded Systems & Sensors
Low power, low bandwidth

Smart Objects

Fig.15.Fog computing-another layer

3) Results of Stealth Test: Traditional anomaly detectiontechniques rely on the deviation of current communication from the features of normal communication. These features include memory consumption, CPU utilization, bandwidth usage, etc. Therefore, to study the stealth of man-in-the-middle attack, we examine the memory consumption and the CPU utilization of gateway during the attack. If man-in-the-middle attack does not greatly change the features of the communication, it can be proofed to be a stealthy attack. For simplicity, we assume the attacker will only replay the data at his or her own computer but will not modify the data.

Firstly, we compare the memory utilization of gateway before and after a video call tunnel is built in our experiment.The results are shown in Figure 8, and the red line in plots indicates the average amount of memory consumption. We can see clearly that man-in-the-middle attack does not largely influence the video communication. In Figure 8(A), the average value is 15232 K Bytes, while after we build the video tunnel on gateway, the memory consumption reaches 15324.8 K Bytes in Figure 8(B). Secondly, we show the CPU consumption of gateway in Figure 9. Based on the results in Figure 9, we can also see that man-in-the-middle attack does not largely influence the video communication. In the Figure 8(A), the average value is 16.6704%, while after the video tunnel is built, the CPU consumption reaches 17.9260%. We therefore conclude that man-in-the-middle attack can be very stealthy in Fog computing because of the negligible increases in both memory consumption and CPU utilization in our experiments.

C. Privacy Issues

In smart grids, privacy issues deal with hiding details, such as what appliance was used at what time, while allowing correct summary information for accurate charging. R. Lu et al. described an efficient and privacy-preserving aggregation scheme for smart grid communications . It uses a super-increasing sequence to structure multi-dimensional data and encrypt the structured data by the homo-morphic cryptogram technique. A homo-morphic function takes as input the encrypted data from the smart meters and produces an encryption of the aggregated result. The Fog device cannot decrypt the readings from the smart meter and tamper with them. This ensures the privacy of the data collected by smart meters, but does not guarantee that the Fog device transmits the correct report to the other gateways.

VI. CONCLUSIONS AND FUTURE WORK

We investigate Fog computing advantages for services in several domains, and provide the analysis of the state-of-the-art and security issues in current paradigm. Based on the work of this paper, some innovations in compute and storage may be inspired in the future to handle data intensive services based on the interplay between Fog and Cloud.

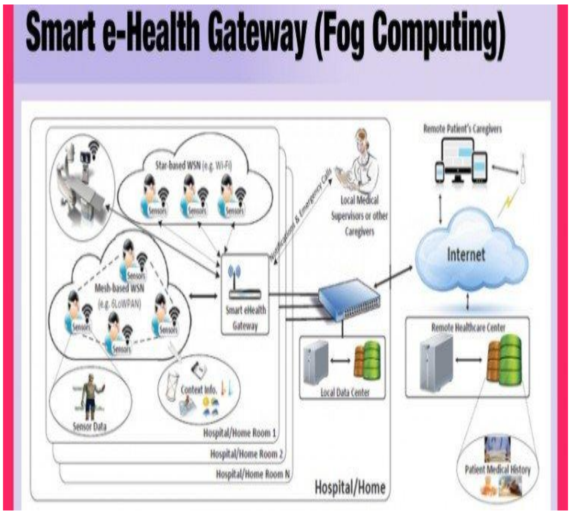

Smart e-Health Gateway (Fog Computing)

Fig.16.Smart e-health gateway

Future work will expand on the Fog computing paradigm in Smart Grid. In this scenario, two models for Fog devices can be developed. Independent Fog devices consult directly with the Cloud for periodic updates on price and demands, while interconnected Fog devices may consult each other, and create coalitions for further enhancements. Next, Fog computing based SDN in vehicular networks will receive due attention. For instance, an optimal scheduling in one communication period, expanded toward all communication periods, has been elaborated in [6]. Traffic light control can also be assisted by the Fog computing concept. Finally, mobility between Fog nodes, and between Fog and Cloud, can be investigated. Unlike traditional data centres, Fog devices are geographically distributed over heterogeneous platforms.

REFERENCES

[1] F. Bonomi, "Connected vehicles, the internet of things, and fog computing," in *The Eighth ACM International Workshop on Vehicular Inter-Networking (VANET)*, Las Vegas, USA, 2011.

[2] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proceedings of the First Edition ofthe MCC Workshop on Mobile Cloud Computing*, ser. MCC'12. ACM,2012, pp. 13–16.

[3] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, Apr 2010.

[4] C. Wei, Z. Fadlullah, N. Kato, and I. Stojmenovic, "On optimally reducing power loss in micro-grids with power storage devices," *IEEEJournal of Selected Areas in Communications*, 2014 to appear.

[5] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[6] K. Liu, J. Ng, V. Lee, S. Son, and I. Stojmenovic, "Cooperative data dissemination in hybrid vehicular networks: Vanet as a software defined network," *Submitted for publication*, 2014.

[7] K. Kirkpatrick, "Software-defined networking," *Commun. ACM*, vol. 56, no. 9, pp. 16–19, Sep. 2013.

[8] Cisco, "Cisco delivers vision of fog computing to accelerate value from billions of connected devices," Cisco, Tech. Rep., Jan. 2014.

[9] K. Hong, D. Lillethun, U. Ramachandran, B. Ottenwälder, and B. Koldehofe, "Opportunistic spatio-temporal event processing for mobile situ-ation awareness," in *Proceedings of the 7th ACM International Confer-ence on Distributed Event-based Systems*, ser. DEBS'13. ACM, 2013,pp. 195–206.

RECENT TRENDS IN TECHNOLOGY (HUMAN-COMPUTER INTERACTION)

N.Abdulla Basha[#1] And P.I.Ayesha Siddiqua[*2]

[#1] Be.Cse, Iv Yr, C.Abdul Hakeem College Of Engineering &Technology, Melvisharam, Vellore
*[*2] Be.Cse, Iv Yr, C.Abdul Hakeem College Of Engineering &Technology, Melvisharam, Vellore*

bashu.smile@gmail.com

Abstract—**The objective of this special introductory seminar is to provide newcomers to Human- Computer Interaction (HCI) with an introduction and overview of the field. The material will begin with a brief history of the field, followed by presentation and discussion of how good application development methods pull on the interdisciplinary technologies of HCI. The topics will include the psychology of human- computer interaction, psychologically-based design methods and tools, user interface media and tools, and introduction to user interface architecture.**

I. INTRODUCTION (*HCI*)

The rapid growth of computing has made effective human-computer interaction essential. It is important for the growing number of computer users whose professional schedules will not allow the elaborate training and experience that was once necessary to take advantage of computing. Increased attention to usability is also driven by competitive pressures for greater productivity, the need to reduce frustration, and to reduce overhead costs such as user training. As computing affects more aspects of our lives the need for usable systems becomes even more important.

II. DESIGNING FOR HCI

Design in HCI is more complex than in many other fields of engineering. It is inherently interdisciplinary, drawing on and influencing diverse areas such as computer graphics, software engineering, human factors and psychology. Furthermore, the developer's task of making a complex system appear simple and sensible to the user is in itself a very difficult, complex task the principles for applying human factors to machine interfaces became the topic of intense applied research during the 1940's, when equipment complexity began to exceed the limits of human ability for safe operation. However, the complexity of computing and of software development projects poses additional demands. An engineering paradigm that is common to many other fields can be generalized to a technical approach for engineering usability in computing systems and is now in widespread use. The paradigm follows an iterative cycle through analysis, design, implementation, and evaluation. Usability engineering structures human factors activity to work within software engineering projects.

Development of usable systems draws on technologies from user interface media, software architecture, process and data modeling, standards, and tools for modeling, building and testing user interfaces. Each can be a topic of research or application. These technologies will be covered in the following sections on the psychology of HCI and the computer science of HCI.

III. METHODOLOGIES

A number of diverse methodologies outlining techniques for human–computer interaction design__have emerged since the rise of the field in the 1980s. Most design methodologies stem from a model for how users, designers, and technical systems interact. Modern models tend to focus on a constant feedback and conversation between users, designers, and engineers and push for technical systems to be wrapped around the types of experiences users want to have, rather than wrapping user experience around a completed system.

Activity theory: Used in HCI to define and study the context in which human interactions with computers take place. Activity theory provides a framework to reason about actions in these contexts, analytical tools with the format of checklists of items that design of any computer system. Users, designers and technical practitioners work together to articulate the wants, needs and limitations of the user and create a system that addresses these elements.

IV. HUMAN-COMPUTER INTERFACE

The human–computer interface can be described as the point of communication between the human user and the computer. The flow of information between the human and computer is defined as the *loop of interaction*. The loop of interaction has several aspects to it, including:

Task environment: The conditions and goals set upon the user.
Machine environment: The environment that the computer is connected to, e.g. a laptop in a college student's dorm room.
Areas of the interface: Non-overlapping areas involve processes of the human and computer not pertaining to their interaction. Meanwhile, the overlapping areas only concern themselves with the processes pertaining to their interaction.

Input flow: The flow of information that begins in the task environment, when the user has some task that requires using their computer.

Output: The flow of information that originates in the machine environment.

Feedback: Loops through the interface that evaluate, moderate, and confirm processes as they pass from the human through the interface to the computer and back.

Fit: This is the match between the computer design, the user and the task to optimize the human resources needed to accomplish the task.

V. INTELLIGENT AND ADAPTIVE HCI

Although the devices used by majority of public are still some kind of plain command/action setups using not very sophisticated physical apparatus, the flow of research is directed to design of intelligent and adaptive interfaces. The exact theoretical definition of the concept of intelligence or being smart is not known or at least not publicly agreeable. However, one can define these concepts by the apparent growth and improvement in functionality and usability of new devices in market.

As mentioned before, it is economically and technologically crucial to make HCI designs that provide easier, more pleasurable and satisfying experience for the users. To realize this goal, the interfaces are getting more natural to use every day. Evolution of interfaces in note-taking tools is a good example. First there were typewriters, then keyboards and now touch screen tablet PCs that you can write on using your own handwriting and they recognize it change it to text and if not already made, tools that transcript whatever you say automatically so you do not need to write at all.

One important factor in new generation of interfaces is to differentiate between using intelligence in the making of the interface (Intelligent HCI) or in the way that the interface interacts with users (Adaptive HCI). Intelligent HCI designs are interfaces that incorporate at least some kind of intelligence in perception from and/or response to users. A few examples are speech enabled interfaces that use natural language to interact with user and devices that visually track user’s movements or gaze and respond accordingly.

Adaptive HCI designs, on the other hand, may not use intelligence in the creation of interface but use it in the way they continue to interact with users. An adaptive HCI might be a website using regular GUI for selling various products. This website would be adaptive -to some extent - if it has the ability to recognize the user and keeps a memory of his searches and purchases and intelligently search, find, and suggest products on sale that it thinks user might need. Most of these kinds of adaptation are the ones that deal with cognitive and affective levels of user activity.

VI. HCI SCOPE

Use & Context: Find application areas for computers Human: Study psychological & physiological aspects e.g., study how a user learns to use a new product, study human typing speed

Computer: Hardware & software offered e.g., input

output devices, speed, interaction styles, computer graphics

Development: Design, implementation & evaluation

VII. HCI GOALS

At physical level, HCI concerns the selection of the most appropriate input devices and output devices for a particular interface or task. Determine the best style of interaction, such as direct manipulation, natural language (speech, writteninput), WIMP (windows, icons, menus, pointers), etc.

- Develop or improve
- Safety
- Utility
- Effectiveness
- Efficiency
- Usability

Appeal of systems that include computers:

□ Safety: protecting the user from dangerous conditions and undesirable situations.

Users: Nuclear energy plant or bomb-disposal – operators should interact with computer-based systems remotely.Medical equipment in intensive care unit (ICU).

□ Data: Prevent user from making serious errors by reducing risk of wrong keys/buttons being mistakenly activated.

Provide user with means of recovering errors. Ensure privacy (protect personal information such as habits and address) & security (protect sensitive information such as passwords, VISA card numbers)

Utility: extent of providing the right kind of functionality so that users can do what they need or want to do.

High utility: Scientific calculator provides many mathematical operations, built-in formulae, and is programmable.

Low utility: Software drawing tool does not allow free-hand drawing but supports polygon shape drawing.

Effectiveness: Concern a user’s ability to accomplish a desired goal or to carry out work.Find a master thesis in our library Web

Efficiency: a measure of how quickly users can accomplish their goals or finish their work using the system. Find a book “human computer interaction” in our library Web. How about a master thesis whose author’s last name is “Cheng”?. How about the newest book in the subject of “human computer interaction”?

Usability: ease of learning and ease of use. Can I use the basic functions of a new digital camera without reading the manual? Does the software facilitate us to learn new functions easily?

Appeal: how well the user likes the system. First impression. Long-term satisfaction Employees in a company perform their jobs in a faster manner. e.g., Workers in a mainland company needed to press a lengthy sequence of buttons in performing a task. An IAS student helped to increase their productivity via writing a batch program for the button pressing operation.

e.g., Intranet can increase employees’ efficiency.

Lowering support costs:

If the product is not usable, calls to customer support can be enormous.
e.g., If a washing machine is difficult to use even after reading the instruction manual, many users will call the customer service and the cost per call can be over $100.

Reducing development cost:

Avoid implementing features users don’t want and creating features that are annoying or inefficient.
e.g., If there are too many unnecessary confirmation dialog boxes in using a word processor, it is likely this product needs to be redeveloped.

VIII. CONCLUSION

The subject of Human Computer Interaction is very rich both in terms of the disciplines it draws from as well as opportunities for research. Discussed here was just a small subset of the topics contained within HCI. The study of user interface provides a double-sided approach to understanding how humans and machines interact. By studying existing interfaces (such as the graphical user interface or the command line interface), we gain an understanding of how the human mind processes information. We gain insight into how human memory deals with the information presented, as well as its limitations. Alternatively, from studying how human physiology and psychology, we can design better interfaces for people to interact with
computers. Work in this domain is only beginning (indeed the number of papers written on this topic has increased in the past few years), and there is much that we don’t yet know about the way the human mind works that would allow more perfect user interfaces to be built.