Asian Journal of Engineering and Applied Technology
ISSN: 2249-068X (P) Vol. 6 No. 1, 2017, pp.23-28

DOI: https://doi.org/10.51983/ajeat-2017.6.1.814

Security Framework for Cloud Based Medical Monitoring System

G.Meera Gandhi[1], J.John Jasper[2] and Emmanuel Andrew[3]
[1]Professor, [2,3]Student, Faculty of Computing
Sathyabama University, Chennai, Tamil Nadu, India
E-mail: professorgandhi29@gmail.com
john.jasper2107@gmail.com, eandrew4738@gmail.com
(Received 5 March 2017; Revised 23 March 2017; Accepted 8 April 2017; Available online 15 April 2017)

Abstract **- Our proposed work helps in developing a framework for cloud based medical system emergency situations, in order to provide a better and feasible service .The main objective of our article is to reach out and help people who are without any access to medical attention or facilities, increase security and maintain regular monitoring of patients by means of which their life can be protected . A new system is designed in such a way that any person can consult a doctor at any time through a smart phone. As a precaution to this problem, bio medical sensors are employed for monitoring the patient's health even in the presence and absence of a health care professional. In this article we are using sensors mainly to measure heart beat, blood pressure and temperature. The sensor values are updated in the server and are available for the doctors to check. Doctors can prescribe medicines and medical advices, which are sent via patient's mobile phone. Various measures like Accuracy, Sensitivity and Specificity are concentrated to verify the performance of the devices employed in the cloud based medical system. Our monitoring system provides efficient and regular monitoring by intimating the doctors for further of treatment .To ensure the safety of patients record Rabin's Algorithm is used for the encryption.**

Keywords: **Security Framework, Cloud, Medical Sensors, Accuracy, Sensitivity, Specificity, Rabin's Algorithm.**

I. INTRODUCTION

Present day developments in communications have used technologies with related computing and digital electronics. These developments permit patient data, which includes vital signs to be surveyed at a distance. Monitoring is done by the use of electronic interfaces and technologies has provided support to health care, when distance separates the doctors from patients in hospital. Depending on patient's condition there will be variation in vitals, so regular monitoring is required. So in our article, Monitoring of vitals is carried by appropriate sensors such as lm 235, kbp500 are used for monitoring the temperature, blood pressure, heart beat of the patient. Bluetooth technology is used to send the information to mobile in turn the details are Sent to stored in cloud. Doctor can check all previous description of the patient and current status of the patient is updated in the server.In the proposed system, a medical kit is designed consisting of blood pressure sensor, temperature sensor, heartbeat sensor are used to keep record of the patient's health.

In this article, monitoring of vitals is carried by appropriate sensors in the medical kit connected to the computer or smart phone. The values from the sensors are received using the help of Bluetooth. The updated values are later then encrypted and stored in cloud server and is accessed by the doctors. Rabin's algorithm is used for the encryption process, because it is faster and lighter than RSA algorithm. An android application is created ,the values are received using Bluetooth. The application helps to create awareness among the users .Based on the values the patients are classified under Healthy, Alarming and Emergency.

Emergency doctors face patients with various situations every day. There are many tests available but the tests with least error and more accuracy are more desirable. Accuracy helps to separate patients from healthy people hence tests with 100% accuracy should be our first choice. But this does not happen in reality as the values varies for different diseases at different situations. Sensitivity is its ability to detemine the patient cases correctly and specificity ability is to determine the healthy cases correctly.

Accuracy: (TP+TN)/(TP+TN+FP+FN)
Sensitivity: TP/(TP+FN)
Specificity: TN/(TN+FP)

(TP) True positive: cases correctly identified as patient.
(FP) False positive: cases incorrectly identified as patient.
(TN) True negative: cases correctly identified as healthy.
(FN) False negative: cases incorrectly identified as healthy

Graphical Illustration

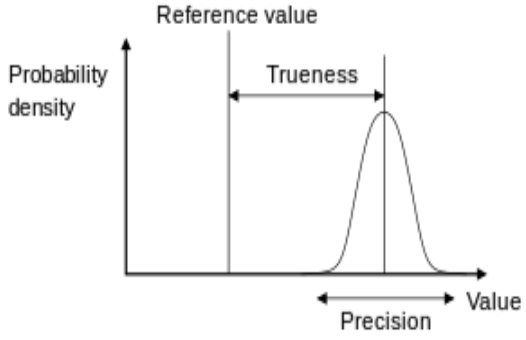

Fig.1 According to ISO 5725-1, Accuracy consists of Trueness and Precision.

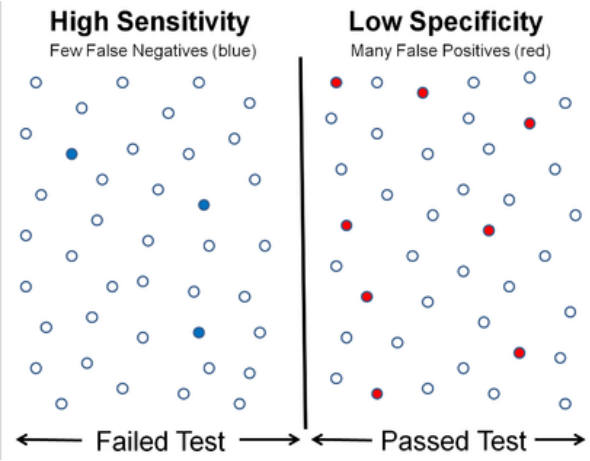

Fig.2 High sensitivity and low specificity

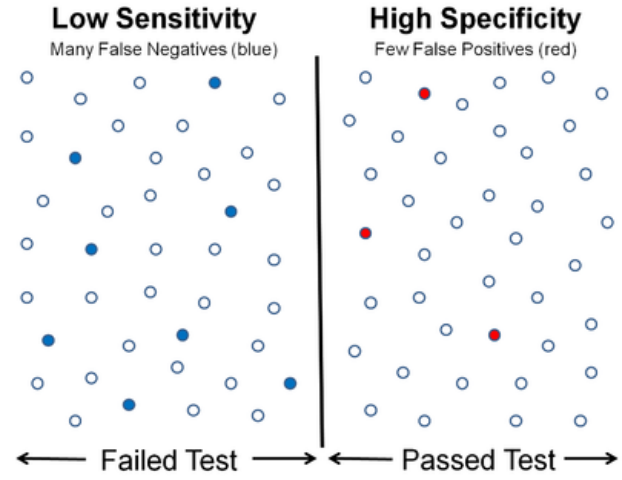

Fig.3 Low sensitivity and High specificity

II. REVIEW OF LITERATURE

In recent years many have strived towards creating better medical facilities for people living in the rural areas. Great initiative steps have been taken towards the helping the people living in rural areas. The existing system consists of a health kit which contains sensors ,wireless connection network, Cloud manager is responsible for managing and controlling all operations between the medical system and cloud. Identity Based Encryption is used for unique user ID enabling data to be protected without the need for certificates. The existing system uses MATLAB to classify the dataset. The conditions and thresholds are used as per the values of Table to design the algorithm for detecting emergency and alarming situation.

The important requirement for the service information is the establishment and improvement of Doctor-patient interaction system. In Implementation of a Cloud-Based Electronic Medical Record , (Uamuzi Bora 2015), i.e. Cloud Medical Report was implemented to improve the service of healthcare system in rural areas." HealthCare Monitoring and Alerting System Using Cloud Computing (Jubi Rana 2015),The authors are implementing a system capable of generating a EMR i.e. Electronic Medical Records of patients which will help in patient's diagnostic and for medical practicing doctors. This system keeps track of patient as well as provide alarming system during emergency.

Rural Health Care Monitoring And Evaluation Using Mobile Cloud Computing Architecture (Rishaw shaw 2014),The authors are implementing a mobile cloud architecture where the patients records are surveyed by VHN(village home nurses) and sms is used as a medium to interact with patients. The authors have also done a comparative study of present health monitoring system and cloud based monitoring system where cloud based approach looked effective. "Cloud based Data Mining framework for monitoring Healthcare in rural India (Vijesh kumar Patel 2015),Proposed a framework that is designed to utilize a private cloud and data mining techniques using ICT (information and communication techniques)". Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-based Processing (mhassan 2015) Opportunities and Challenges reviewed the present state and future integration of remote health monitoring technologies with sensors(wearable) equipped with IoT intelligence .They have used certain sensors to check the Health Conditions related to Diseases such as Cardiovascular Disease (CVD), Chronic Obstructive Pulmonary Disease (COPD) etc..

Cloud Care: A Remote Health Monitoring System(R.Deepa 2014) ,Implementing for end-to-end solutions that facilitate continuous access to health care information enabled by remote sensing smart systems and ubiquitous telecommunications networks. Design and Implementation of a Cloud Based Rural Healthcare Information System Model (RP Padhy 2015),Provided a model where use of sensors are limited according to the cost, patients can view their health report on request basis and the disadvantage is lack of security and communication. Low Cost and Portable Patient Monitoring System for e-Health Services in Bangladesh(Mithun Chandra Paul 2016),This paper proposes portable patient monitoring system and low cost for e-Health services using a raspberry pi microcomputer for collecting data from different sensors.

"SPHPMS: Smart Personnel m-Healthcare Patient MonitoringSystem(Hoda Ramin Hossein 2016),the authors are using NFC technology where the NFC encoded devices is being used to read the information from patients .They have also used web server in this model for storing the sensitive data of patients. They have avoid using Servlets because it only allows clients (Java technology) to be interfaced, but web server architecture allow all clients of other technologies to be interfaced, but it needs to be in constant contact (physically touched) with each other ,which is not always possible.

Telemedicine approach for Remote Patient monitoring system using smart phones with an economical hardware kit (Syed Thouheed Ahmed S, 2016),The proposed system was designed for people who suffer from hypertension and hypotension .It is programmed to capture pre-cardiac arrest .Biomedical sensors and photo-electronic sensors are being used but Biomedical sensors are costly and photoelectric sensors need shiny surface to work on. An Iot Based Patient Monitoring System Using Raspberry Pi (Dr.M.Pallikonda Rajasekaran 2013),Efficient Monitoring System for Cardiac Patients Using Wireless Sensor Networks (WSN) (Vijayashaarathi S 2016),Wireless Sensor Based Handy Patient Monitoring System((Neha R. 2016), proposed reading of health data using ARM cortex M3 Processor and the read values are sent to the doctor's mobile via GSM(Global System for Mobile Communications) but the disadvantage is that ARM cortex M3 processor is 32 bit and the processor is costly which can not be provided by rural people. The monitoring of patients is carried in particular time that is the periodic rounds other than no one care about patient, so full day monitoring is not possible. Relation of patient will there for helping patient they don't know what to do during emergency .Data base of patient record is not maintainedproperly. If some hospital having manual database in written format there is difficult to find exact one.

Privacy Protection for Wireless Medical Sensor Data (Xun Yi 2016),Implemented a system to securely distribute the patients data in multiple servers.And to perform analysis on the patient's data without affecting their privacy Paillier and ElGamal cryptosystems are used. FPGA Implementation of Advanced Health Care system using Zig-Bee enabled RFID Technology (Joyashree Bag 2014),proposed a system to integrate the developed Zig-enabled RFID processor which will be very accurate,fast and cost efficient.Coexistence of ZigBee-Based WBAN and WiFi for Health Telemonitoring Systems (Yena Kim 2016),implemented an algorithm to control the load in WiFi networks to assure the delay requirement for physiological signals, especially at emergency situations where there's a coexistence of ZigBee-based WBAN and WiFi.

III. METHODOLOGY

This paper involves client-server architecture The server stores data from patients and sends it to the doctors sever. The doctor monitors the signal information from patient. Figure 5 display the flow chart of the proposed system. The proposed paper discusses five main components.The architecture is divided into 5 parts: *A. Biomedical Sensors; B.Architecture and hardware. C. Security D. Database and E. Application.*

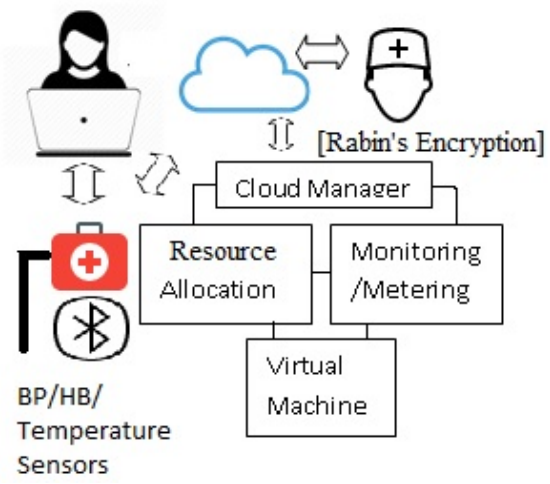

Fig.4 Framework for Patient Monitoring System

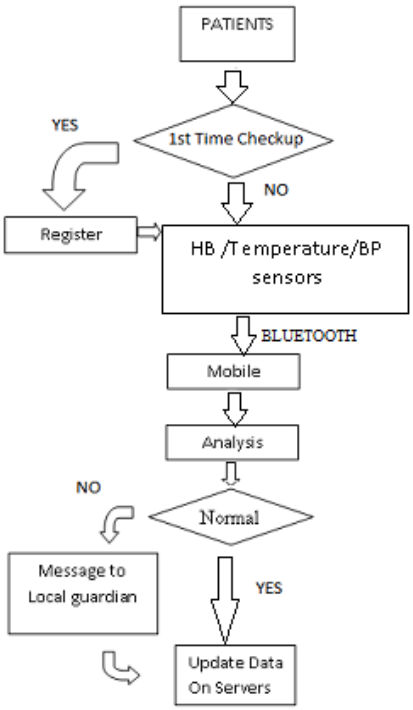

Fig.5 Flowchart of the proposed System

A. HealthCare Sensors

Various medical sensors are employed like blood pressure sensor, temperature sensor, heartbeat sensor. In order to send the sensor data of every patient through mobile automatically, sensors are connected with a microcontroller

Kbp500 measures the pressure level of the blood. It Shows Systolic, Diastolic and Pulse Readings. Compact design fits over your wrist like a watch. The diastolic reading, is the pressure in the arteries when the heart rests between beats. Its during this time when the heart fills with blood and gets oxygen. A normal diastolic blood pressure is lower than 80.90 or higher is high blood pressure. In blood pressure reading, the systolic number comes first, and then the diastolic number. For

example, fig(b) your numbers may be "120 over 80" or written as 120/80. Compact design fits over your wrist like a watch.

Heart Beat sensor monitors the heartbeat. The digital output connected to the microcontroller to measures the (BPM) Beats Per Minute rate. It works on the principle of light modulation by which blood flow through finger at each pulse.

TABLE 1 BLOOD PRESSURE READING CHART

Blood Pressure Conditions	Systolic/Diastolic pressure(mm Hg)
Hypertension Stage 4	210/120
Hypertension Stage 4	180/110
Hypertension Stage 4	160/100
Hypertension Stage 4	140/90
High normal blood pressure	130/85
normal blood pressure	120/80
Low normal blood pressure	110/75
Boderline hypotension	90/60
Serious hypotension	60/40
very Serious hypotension	50/33

TABLE 2 HEART BEAT /AGE CATEGORY (BPM) –PERFORMANCE

	Age(Years)/BPM					
Rating	**18 -25**	**26-35**	**36-45**	**46-55**	**56-65**	**66+**
Excellent	50-76	51-76	49-76	56-82	60-77	59-81
Good	77-84	77-85	49-76	56-82	60-77	59-81
Above Average	85-93	86-94	89-98	94-101	95-100	93-102
Average	94-100	95-102	99-105	102-111	101-109	103-110
Below Average	101-107	103-110	106-113	112-119	110-117	111-118
Poor	108-119	111-121	114-124	120-126	118-128	119-126
Very Poor	120+	122+	125+	127+	129+	127+

A normal resting heart rate for adults ranges from 60 to 100 beats a minute. Generally, a lower heart rate at rest implies efficient heart function and better cardiovascular fitness. Taking an athlete for an example, a well-trained athlete might have a normal resting heart rate closer to 40 beats a minute. To measure your heart rate, pulse is checked by keeping index and third fingers on the patient's neck to the side of their windpipe. When pulse is felt, count the number of beats in 15 seconds. Multiply this number by 4 to calculate beats a minute.(BPM)

Factors can influence heart rate, includes:

1. Activity level
2. Fitness level
3. Air temperature
4. Body position
5. Emotions
6. Body size
7. Medications

Temperature Sensor monitors the temperature of the patient. All the values are stored to the cloud where cloud manager takes care of transferring the data. LM35 Sensor measures body temperature of patient which is capable of self-heating . The LM35 is operates over a −55˚ to +150˚C temperature range.

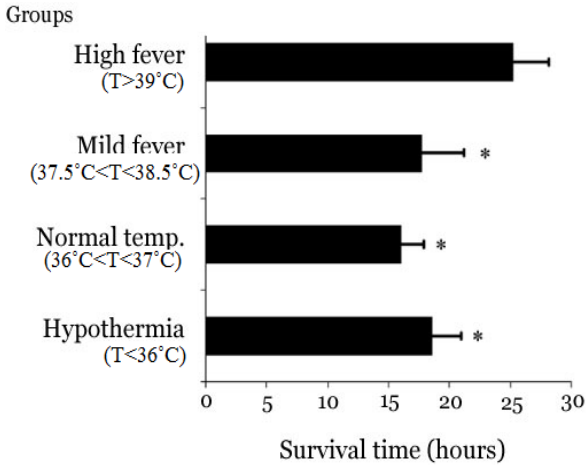

Fig.6 Fever temperature chart

B. Architecture and hardware

PIC 16F877A Microcontroller. It is a High performance RISC CPU machine. 28 bit timer and one 16 bit timer is available 10bit multi-channel A/D converter Synchronous Serial Port (SSP) with SPI (master code) and I2C.

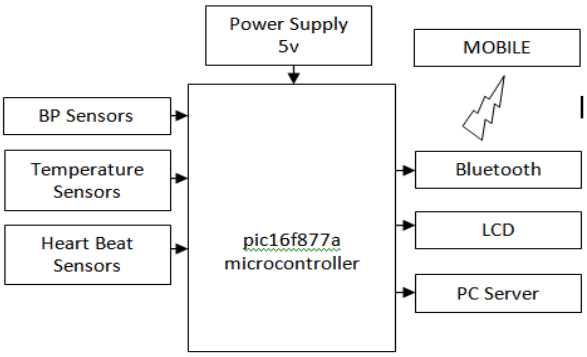

Fig.7 Block diagram of Patient Monitoring System

MAX232 converts TTL into RS232 logic level converter used between the microcontroller and the GSM board or PC. Communication between Bluetooth devices happens over short-range, ad hoc networks known as piconets.

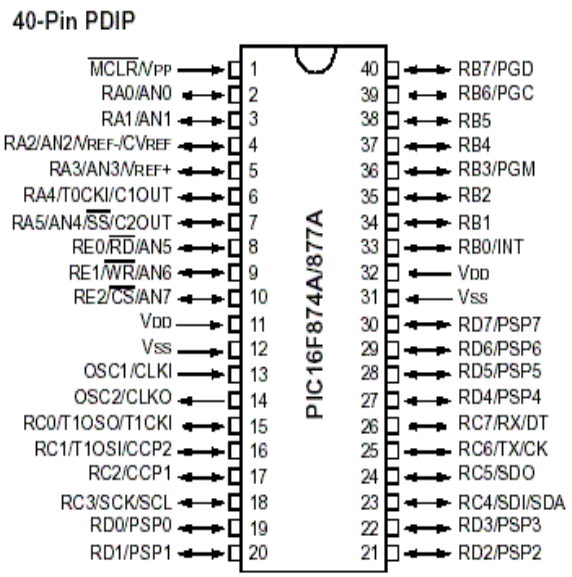

Fig.8 PIC16F874A/877A

The MAX232: two drivers that convert from TTL logic to RS-232 voltage levels as well as two receivers that convert from RS-232 to TTL voltage levels,. As a result, only two out of all RS-232 signals can be converted in each direction. Typically, the first driver or the receiver pair of the MAX232 is used for TX and RX signals, and the second one for CTS and RTS signals.

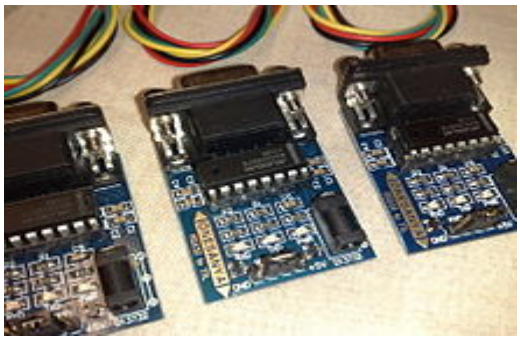

Fig.9 MAX232

A piconet is a network of devices connected using Bluetooth technology. Piconets are established dynamically and automatically as Bluetooth devices enter and leave radio proximity. The program is written in EMBEDDED 'C' language and is compiled by HI-TECH C compiler using MPLAB IDE software. The compiler is used to convert middle level language into machine level language. After the 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 theprogram is burnt into the ROM (Flash memory) of PIC16F877A by using PICKIT2 Programmer.

C. Security

For secure authentication, we are using Rabin authentication algorithm to secure the signature of an user for the safety of the data from the sensors to the medical staff..Rabin's algorithm is considered to be lighter and faster compared to RSA, Rabin system use a pubic and a private key where private key is only by the recipient. The precise key-generation process follows:

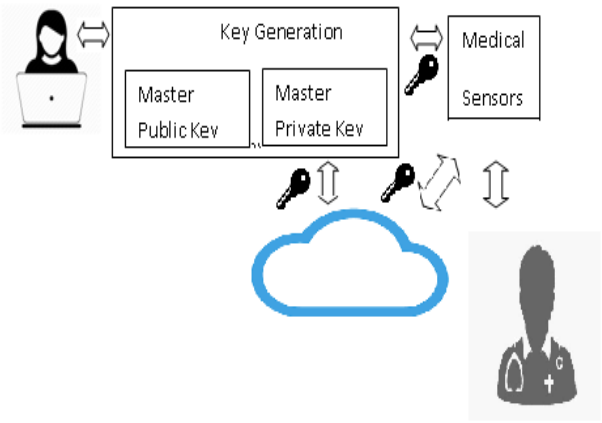

Fig.10 Security Encryption Scheme

Select two distinct large primes a and b. One may choose a=b=3 (mode 4) to simplify the computation of square roots modulo p and q. The scheme works with any prime numbers.

Let n=a.b ,where n is the public key. The primes a and b are the private key.

During encryption , the public key is required and to decryrpt the factors of a and b are necessary.

1.Encryption: of the plaintext w<n

$$C=w^2 \bmod n$$

2.Decryption: using a method to compute w given c with Chinese remainder the one can get that w equals to one of the numbers :

$w_1 = c^{(p+1)/4} \bmod n$ $w_2 = a\text{-}c^{(p+1)/4} \bmod n$

$w_3 = c^{(q+1)/4} \bmod n$ $w_4 = b\text{-}c^{(q+1)/4} \bmod n$

Indeed, it is easy to verify , using Euler's criterion which says that if c is a quadratic

Residue modulo p, then $c^{(p-1)/2}=1(\text{mod } a)$, that

$\pm c^{(p+1)/4} \bmod a$ and $\pm c^{(q+1)/4} \bmod b$

Are two square roots of c modulo a and b

The Rabin algorithm is generally based on blocks of 512 bits, or 1024 bits, or 2048 bits, of which the last 64 bits consist of padding which gives a payload of 448, 960 or 1984 bits (56, 120 or 248 bytes), respectively; sometimes a padding of 128 bits is used, if there is some concern about

the possibility of a false duplicate. Another method used pads the message with 64 0-bits (or 128 bits instead of 64 bits, or 1-bits instead of 0-bits), so that only the square root with the desired pattern is used. The message is split into blocks of the required size and is extended by adding a 1-bit followed by 0-bits.

D. Database

Based on the value the patients are classified under Healthy , Alarming and Emergency. During each stage the doctor interacts with the patient through the app giving medical advices.

E. Applications

An android application is created ,the values are received using Bluetooth. The application helps create awareness among the users. During each stage the doctor interacts with the patient through the app giving medical advices. The application also comes with a video calling option where interaction between the patient and doctor becomes easy. Emergency support is also provided ,that is when the values come under alarming or emergency stage an alarm option is fixed to alert the guardian. During this case ,the application also directs the patient to the nearby hospitals and medical advices are also given.

IV. RESULTS AND DISCUSSION

A. Registration

We are creating a user application by which the user is allowed to access the data from the Server .The user has to create a login which helps with the security. The login gives access to the medical database of the patient .The patient is given an unique ID

B.Server

The Server will monitor the entire Users information in their database and verify them if required. Also the Server will store the entire Users information in the database. Server establishes a connection to communicate with the Users. The Server will update the each users activities in the database and the server will verify each user before they access the Application. So that the Server will prevent the Unauthorized Userfrom accessing the Application.

Fig.11 Product

V. CONCLUSION

This paper proposes a new algorithm ie, Rabin's algorithm that deals lighter and faster security of the database. We are using Bluetooth technology to send the info of any abnormalities and the general details of the patient to the server PC. We are enhancing the security of the medical kit using rabin's algorithm. To provide an application this directs patients to the nearest hospital and a video calling option to interact with the doctors during emergency. To make it cost efficiency to user especially in rural areas.

REFERENCES

[1] Olutayo Boyinbode and Gbenga Toriola (2015), "CloudeMR: A Cloud Based Electronic Medical Record System" , International Journal of Hybrid Information Technology Vol.8, No.4, pp. 201-212.

[2] Jubi Rana, Abhijeet Bajpayee (2015) ,"HealthCare Monitoring and Alerting System Using Cloud Computing" International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Vol, 3 No. 2, pp. 102– 105

[3] Rishav Shaw, R.Rajkumar (2014) , Rural health care monitoring and evaluation using mobile cloud computing architecture" International Journal of Advanced Scientific and Technical Research , Vol6 No.4.

[4] Vijesh kumar Patel (2015) ,"Cloud based DataMining framework for monitoring Healthcare in rural India" International Journal ofComputer Science & Engineering Technology (IJCSET), Vol. 6 No. 4

[5] Ms. Hoda Ramin Hossein, Prof. S.S.Shaikh (2016), "SPHPMS: Smart Personnel m-Healthcare Patient Monitoring System, (ICEEOT)

[6] Syed Thouheed Ahmed S, K.Thanuja,(2016),"Telemedicine approach for Remote Patient monitoring system using smart phones with an economical hardware kit " IEEE

[7] Puvaneshwari S, Vijayashaarathi S (2016),"Efficient Monitoring System for Cardiac Patients Using Wireless Sensor Networks (WSN)" IEEE WiSPNET

[8] Neha R, Pandya Vitthal et al., (2016),"Wireless Sensor Based Handy Patient Monitoring System" 2016 IEEE 6th International Conference on Advanced Computing IEEE 6th International Conference on Advanced Computing

[9] Xun Yi, Athman Bouguettaya, et al.,(2016),"Privacy Protection for Wireless Medical Sensor Data" IEEE transactions on dependable and secure computing, vol. 13, no.pp..

[10] Yena Kim et.al (2016),"Coexistence of ZigBee-Based WBAN and WiFi for Health Telemonitoring Systems", IEEE Journal of biomedical and health informatics, Vol. 20, No. 1, pp.

[11] Joyashree Bag,Subhashis Roy, *et al.*, (2014),"FPGA Implementation of Advanced Health Carevsystem using Zig-Bee enabled RFID Technology".