International Journal of Engineering & Technology, 7 (2.33) (2018) 261-265

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

An effective cloud based personal emergency response system by providing privacy protection for the medical data

V. Brindha Devi [1] *, Lokeswari.U [2], Saraswathi.B [2], Vindhya.T [2]

[1] Associate Professor, Sri Sairam Institute of Technology
[2] Sri Sairam Institute of Technology
**Corresponding author E-mail: i4it053@sairamit.edu.in.*

Abstract

Timely access to the emergency medical services is challenging tasks due to the increasing percentage of population. Especially pre-hospital emergency situations are neglected for quite a long time. The agglomeration of medical gadgets and other system applications that bridges the gap to healthcare IT systems through Internet or computer networks is placed under the domain (IoMT) Internet Of Medical Things . In this project an efficient medical data monitoring and an emergency response system has been developed. IoT in healthcare is made to bridge the gap by providing the connectivity through internet making sure that the information is secured and available on the timely access. The wireless monitoring device collects data from various sensors, which is shared into the database using ZigBee cc2530 Transmitter Receiver through UART communication. The wireless device is embedded with sensors like Pulse oximeter (senses the heart beat rate and blood oxygen concentration)and temperature sensor. This data is monitored regularly and if there is any abnormality in the values then an alert is sent to the doctor to intimate the condition of the patient. This paper provides an interaction of the patient with the doctors. The interaction is enabled using public and private chat application where any number of patients can interact with a doctor. It is challenging task to personalize specific healthcare data i.e. medical records for various application users in an appropriate and secured fashion. Thus, the patient's health records i.e. prescription, scan reports, etc. are uploaded by the patient which can be viewed by the doctor. These files are encrypted using an encryption algorithm before uploading it into the cloud. Similarly it is decrypted while downloaded by the doctor for reference. The data collected is used for the prediction of diseases like heart attack and the report is sent to the doctor. Hence the project's aim is, when the recorded value exceeds the threshold range, an automatic intimation with the patient's collected data is sent to the concerned doctor.

Keywords: *Medical Data Sharing; Intrusion Avoidance; Wearable Device; Emergency Responders; Heart Disease Prediction ; Wireless Monitoring Device*

1. Introduction

Medical data monitoring includes collection of the patient health details and their Pulse rate , temperature ,pressure level etc. as source from which the patient can be provided treatment with reference to their previous health condition. The data can be dynamically collected from the wireless monitoring device so that the health condition can be monitored regularly. The disease of a patient is initiated from symptoms like temperature rise etc. Thus detection of these minute details of the patient continuously helps us to predict the disease in advance and check with the doctor. This monitoring system has been developed into a wearable device where the data is transmitted and stored in database from there it is shared to cloud. So far, these data are being collected to just monitor and also for future medical reference about that patient. But the patients don't get to know about the symptoms that may occur due to these variations in the data. Thus, in this paper we provide an interaction of the patient with the doctors in the cloud. However it is challenging issue to personalize specific healthcare data for various users in convenient fashion. Thus, the data collected from the device is encrypted using encryption algorithm and decrypted when viewed by the doctor. The patient and doctor can interact with each other by Public and Private chat application. The patient give their symptoms, with reference to these symptoms & conditions, we update them with articles, news feeds and some health tips. They will also be provided with a tracking facility through which they can find a route to the nearby hospital. This collected data is used in an efficient way by estimating its threshold levels. If the value in the data exceeds the threshold level then it causes an alert to the doctor and the respective persons.

2. Related work

With the advancement in the healthcare, cloud computing, big data and wearable technology there is an crucial need to satisfy the individuals day to day need in monitoring their body conditions regularly. The existing paper [1] describes about the various problems like protection of users personal data while transferring them from the wearable device to the cloudlet ,protection of the entire application from malicious attacks.

In the cloudlet based healthcare system the user's physiological data's privacy and efficient data transmission strategies are required. NTRU algorithm is used for data protection while data

transmission takes place in the cloudlet and the user's similarity level and reputation is measured to build the trust model. Depending upon the user's trust level the system determines whether the data sharing is performed. This paper proposes an collaborative model for the cloud environment based on distributed IDS and Intrusion Prevention System.

The Collaborative IDS (CIDS) based on cloudlet mesh structure is previously studied in Shi et al [2]. The trusted authority (TA) is assigned by the hospital. The two main tasks done by the TA are to measure the trust level of the users and compare the similarity of trust level between the users.

The medical data is encrypted using ONTRU algorithm which is proposed by Thwe Ngwe et al[9]. The abnormal values of the ECG recording obtained is prompted as an emergency intimation to the care taker as proposed by Larkai et al[8].Yong lin et al[10] came up with the concept of Integrated platform setup and multi agent interaction between the caretaker, patients, doctors . Omar S. Alwan et al [6] proposed a real time monitoring of patient's temperature and heart beat using ZigBee module.

3. System framework

3.1. Hardware

The wireless monitoring device consists of Arduino -Mega AT-Mega and a ZigBee cc2530 transceiver module that are fixed in Arduino through the ZigBee shield [6]. These sensors are used to monitor the real time health condition of the patients. This data is transmitted to the database using ZigBee cc2530 as transceiver to transmit the data from the monitoring device.

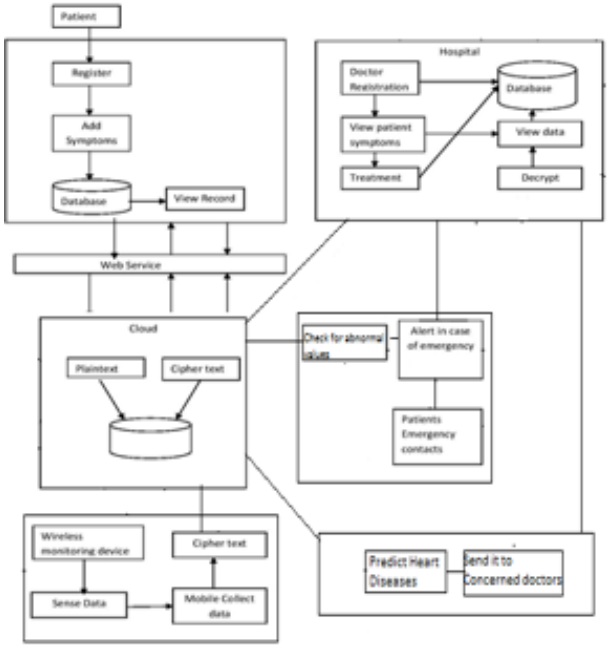

Fig. 1: Architecture Diagram

- Arduino ATmega328: The Arduino Uno is a microcontroller board based on the ATmega328 (datasheet). It is equipped with 14 digital input/output pins. Out of these 14 pins 6 can be used as analog inputs and 6 as PWM outputs. It utilizes 16 MHz crystal oscillator, a USB connection, a power jack, an ICSP header, and a reset button. Its operating voltage is 5V and clock speed is 16MHz.
- ZigBee cc2530 Transceiver: The Zigbee cc2530 can transmit up to the range of 250m. It is a 2.4-GHz IEEE 802.15.4 Compliant RF Transceiver which can transmit a frequency of about 32-kHz. It has an excellent receiver sensitivity and robustness to interference. The additional features are accurate digital RSSI/LQI; the programmable output power may range up to 4.5 dB and needs a wide supply-voltage of range (2 V–3.6 V).
- The LM35 temperature sensor: LM35 Temperature Sensor is Calibrated Directly in ° Celsius (Centigrade). It has a Linear + 10 mV/°C Scale Factor and provides an accuracy of up to 0.5°C (at +25°C). It records the temperature level for a range of about −55°C to +150°C .Its main features are: It is suitable for Remote Applications, cost is low due to wafer-level Trimming and Operation voltage is from 4 to 30 V.
- Generic MAX 30100 Pulse Rate Oximeter:
  The Pulse Oximeter is used to measure both the Heart beat rate and Blood Oxygen Concentration (BOC) The BOC is measured in mmHG units. A pulse oximeter has a main purpose to measure the oxygen saturation in the blood .This sensor consists of two LEDs which emits light to pass through the finger. One light is a Red Spectrum (650nm) and the other one is an Infrared(950 nm). This sensor can be placed anywhere like finger , ear lobe where the light can penetrate through the tissue easily. When both the rays are penetrated through the tissue , the absorption is measured with a photodiode. Based on the ratio of absorbed light and IR light will be compared for the calculation of oxygen in your blood.

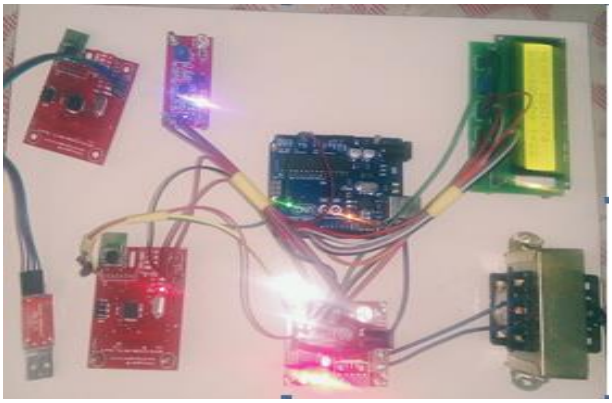

Fig. 2: Wireless Health Monitoring Kit.

- GPS- This is used to send the patient's location in case of emergencies.

3.2 User's data encryption

The User's data is being encrypted using Optimized NTRU algorithm contributed by Thwe Ngwe et al. [13] which is more efficient than AES, Diffie Hellman and other encryption schemes. In ONTRU the admin creates a digital envelope i.e. message encryption using AES algorithm and secret key encryption using ONTRU studied in [9]. This digital envelope system combines the symmetric key algorithm and asymmetric key algorithm in order to provide security requirement such as confidentiality.

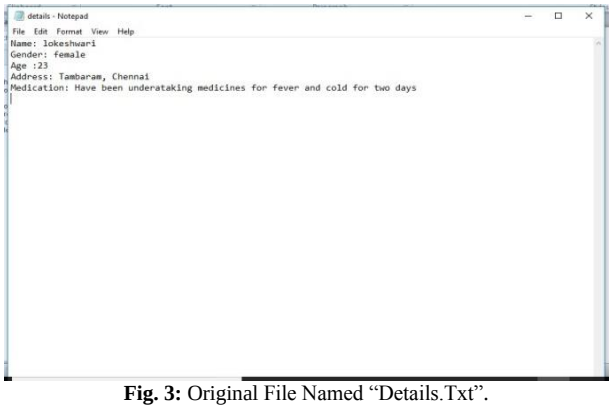

Fig. 3: Original File Named "Details.Txt".

The ONTRU is much more efficient than NTRU where it uses a polynomial ring. But in ONTRU it uses a matrix formulation. f1 = I + pf Where I is the identity matrix which is used for the matrix formulation.

Table 1: Encryption by Ontru Algorithm

Components	NTRU(by using truncated polynomial ring)	ONTRU(by using matrix formulation)
Key Generation	1) Private Key is (f, fp). 2) fp= f-1 (mod p) 3) 3. Public key is h = p*f*q * g (mod q)	1. Private key is f1 2. f1= I + pf 3. Public key is H=p*(f1)q*g (mod q)
Encryption	e = rand * h + m (mod q)	1. E = rand * H + m (mod q)
Decryption	1) f * e (mod q) 2) a (mod p) 3) fp * b (mod p)	1) f1 *E (mod q) 2) = a (mod p)

The parameters used in this algorithm represents:
N - The numbers of entries in the matrices.
q - The large modulus to which each entries in the matrices is reduced.
f - A matrix that is the private key.
p- The small modulus to which each entries in the matrices is reduced.
g - A matrix that is used to generate the public key h from f.
h - A matrix that is the public key.
Rand - the random matrix.

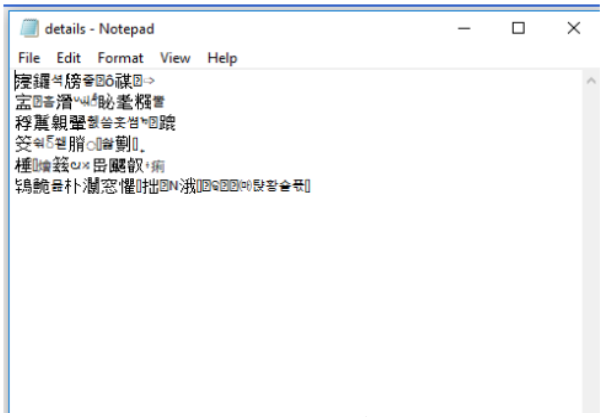

Fig. 4: The Encrypted Format of the Original File.

The steps by which the medical records are encrypted is as follows:

- Initially the file is encrypted using a symmetric algorithm i.e. using AES algorithm.
- Thus, it produces a secret key and an encrypted file.
- The secret key is further subjected to encryption. The secret key is encrypted using ONTRU encryption algorithm.
- This encrypted secret key and the encrypted file is sent to the receiver.
- At the receiver end the secret key is first decrypted and the encrypted file is decrypted using the decrypted secret key i.e. the private key of the sender.

3.3. Patient health records upload in cloud

Due to the rapid development of Cloud and the use of wearable devices, the Patient's health records are preserved in a more secured way. It also provides as a backup copy, which cannot be erased or disrupted. The patient can upload their health records like ECG reports, Scan reports, or other prescriptions. These records are uploaded to Cloud platform, here we use Cloud Me file storage service which is operated by a secure European Service Cloud Me AB.
Cloud Me is a Cloud storage platform and a way to sync folders that authorize the users to store, access and share their content, both with the other user of Cloud Me and also with user outside the Cloud Me sync/storage service.

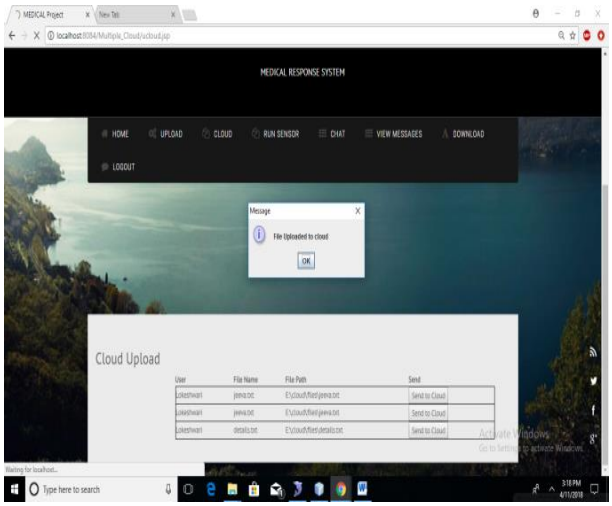

Fig. 5: File Upload to Cloud.

The uploaded records are encrypted using encryption algorithm and it is shared to the doctor. The Doctor can view all the files shared by the patient with the patient's name.

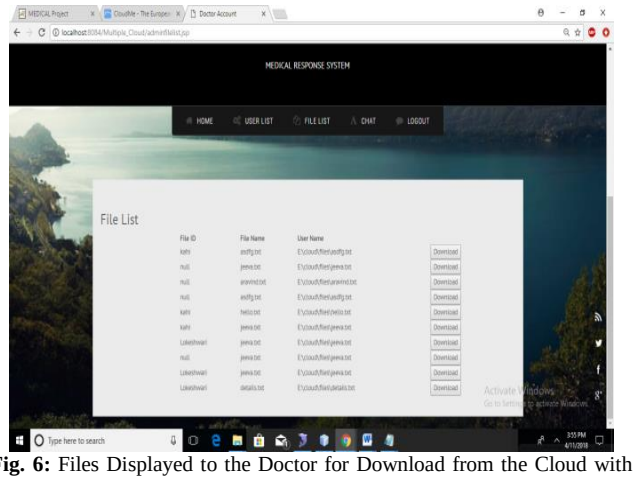

Fig. 6: Files Displayed to the Doctor for Download from the Cloud with the Appropriate Patient Name.

These records can be downloaded by the Doctor after decryption by the same AES decryption algorithm for future reference. Only the authenticated Patient and Doctor can view those records. These data will be stored only in a encrypted format in the cloud so that no one can view those records which will be preserves with security.

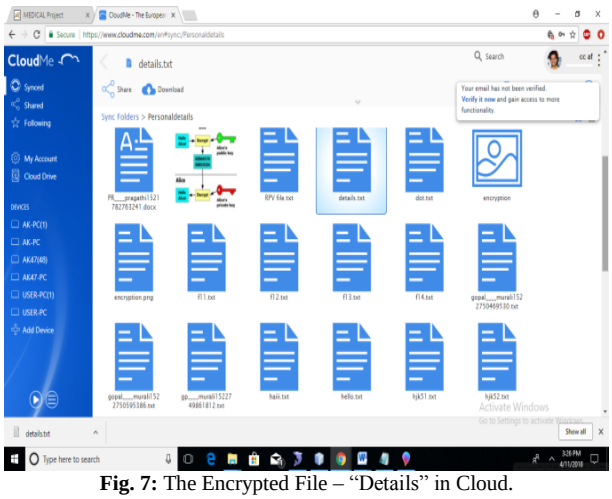

Fig. 7: The Encrypted File – "Details" in Cloud.

3.4. Intrusion avoidance system

The main issue of cloud based medical data collection is the security and the intruders or attackers. Thus Intrusion avoidance system is used to deter the intruders. The attacks are detected and avoided using Intrusion avoidance system. In this, the detection rate and false alarm rate are plotted as the receiver operating characteristic (ROC) curves. Further the collaborative detection rate is analyzed and expected cost of implementation in the cloud is estimated. The user's data is collected as two identifiers EID and MI as studied in [1]. The EID consists of the Patient's unique identifier and their personal health details. The MI consists of medical information like symptoms, treatment, etc. We use a Trust Authority level to share the data from the database to the cloud where the User's trust level is compared with the threshold level. With the increase of reputation and similarity, trust level of user will be improved.

- Gaussian function is selected as the corresponding function, which will map the value in the collection into a trust level.
- Formulate the relevant guidelines and have the experts set up the trust-related guidelines with the related reputation and similarity.
- After obtaining users' trust level, we can judge whether to trust user 'a' based on threshold value set by user 'b', where 'b' is the patient.
- If the trust level is greater than or equal to the threshold value, then the user a can be trusted, so TA will share user 'b' information to user 'a', where 'a' is the doctor.
- If the trust level is less than the threshold value, then the user 'a' cannot be trust, so TA will refuse the request of the user 'a'.

3.5. Patient and doctor interaction

The doctor and the patient can interact with each other via Public and Private Chat.

- In Private chat, the patients are facilitated to send their symptoms and ask suggestions to their concerned doctor.

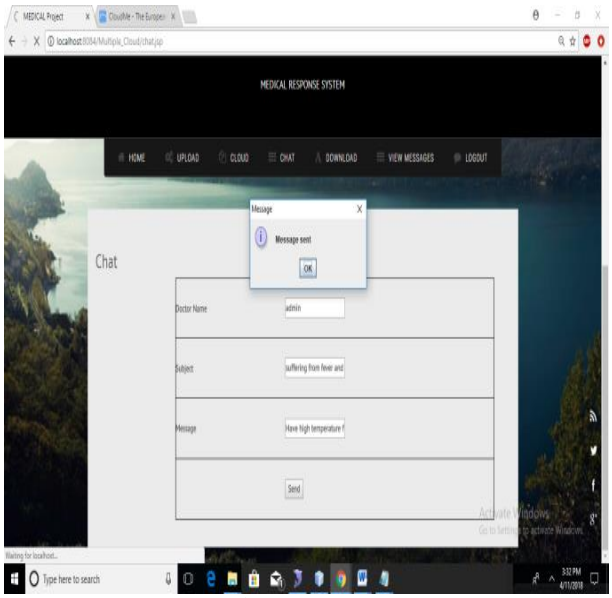

Fig. 7: Patient's Message to Doctor.

- In Public chat, the doctor can view chat messages of many patients at a time. So the doctor can give opinion or health tips to all the patients.

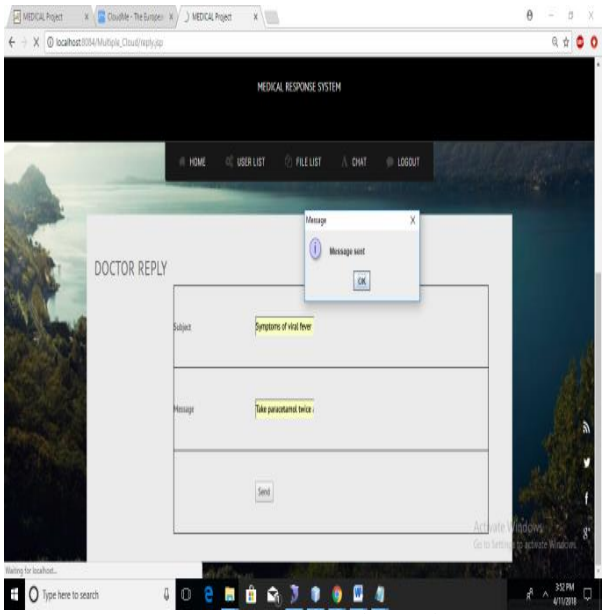

Fig. 8: Doctor's Reply to Patient.

3.6. Alert based personal emergency response system

This dynamic measurement of heart rate , temperature, oximeter and blood pressure level, with the goal of patient state estimation and clinical outcome prediction. The Patient's data is estimated according to the time series. The estimated data is evaluated with the threshold level.

This is used to evaluate the current data with the threshold level to send alerts and the complete information of the patient medical records to the doctor, patient's relatives and the hospital. The Patient's location is also sent to the hospital from the GPS embedded in the monitoring device.

- The threshold values are fixed according to the data collected. These are the average values which are meant only for a normal human being.
- They are-the heart beat range varies from 60 to 100 beats/min.
- The blood pressure range varies as More than 120 over 80 and less than 140 over 90 (120/80-140/90).
- The Pulse oximeter range should be 95 to 100 percent. The human temperature range should be 36.5–37.5 °C (97.7–99.5 °F).

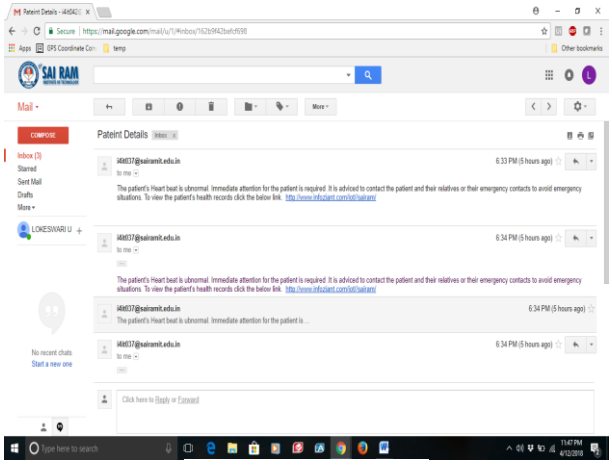

Fig. 9: Alert Mail to Doctor.

- The intimation of alert is sent to the doctor through the email along the URL link which contains the patient's recorded values. The mail is configured through an SMTP protocol.

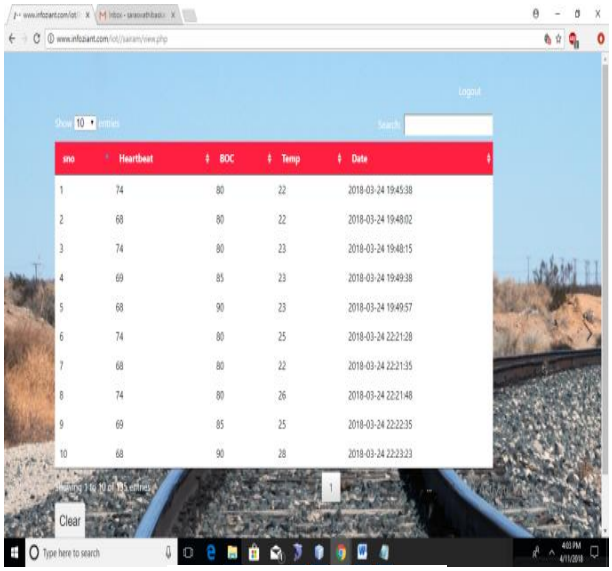

Fig. 9: Recorded Values in URL

- If all the obtained data exceeds below or beyond the threshold level, then the alert will be prompted to the doctors, patient's emergency contacts and to the nearby hospital.
- These heart beat rate collected so far are plotted in a graph for the representation to the doctor during treatment of patient. This also provides a predicted report which is reported for every 40 values of the data.

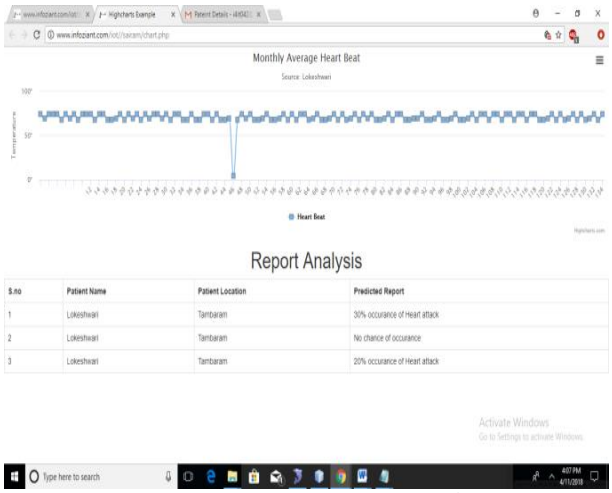

Fig. 10: Predicted Report and Plotted Graph of Heat Rate.

- The data collected so far is sent to the doctor through an URL along with the alert message. The doctor can view the monitored values of the patient from wherever they are through the URL.

4. Conclusion

In this paper we have investigated the problems faced in sharing large medical data in cloud and privacy protection. This paper proposes to protect the medical data of the users through encryption techniques and Cloud is further used for the storage of patient's health records. The cloud allows only patients and doctors to view the encrypted data. This project utilize the wireless health monitoring devices to collect user's data and for privacy protection ONTRU mechanism is used which ensures that the user's transmitted data are secure in cloud. This uses an alert mechanism for intimation of patient's location and details in case of emergency to the doctor, hospital or emergency contacts.

In future advancements an automatic tracking system can be developed which can identify and track the patient's to the nearby hospitals for both consultation and in case of emergency situation. An application can be developed for prediction of the other diseases with the patient's symptoms and providing them with health tips and suggestions based on their body conditions.

References

[1] Base paper - Min Chen, *Senior Member, IEEE*, Yongfeng Qian, Jing Chen, Kai Hwang, *Fellow, IEEE*, Shiwen Mao, *Senior Member*, Long Hu "Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing" published in IEEE Transactions on Cloud Computing, 2017.

[2] Andrews Samraj, Kalvina Rajendran "Communication by Gestures in Personal Emergency Response System" published in Emerging Trends and Applications in Computer Science (ICETACS), 2013 1st International Conference.

[3] Arbish Akram, Maria Anjum, Mariam Rehman, Hafsah Bukhary, Hifza Amir, Rafia Qaisar - "Life Savior: An Integrated Emergency Response System" published in Information Technology (ICIT), 2017 8th International Conference.

[4] R. Bye, A. Camtepe and S. Albayrak. "Collaborative Computer Security and Trust Management", Chapter Teamworking for Security: The Collaborative Approach, Information Science Reference, 2009.

[5] K. Dongre, R. S. Thakur, A. Abraham *et al.*, "Secure cloud storage of data," in Computer Communication and Informatics (ICCCI), 2014 International Conference on. IEEE, 2014, pp. 1–5.

[6] David L Larkai, Ruiheng Wu -"Wireless Heart Rate Monitor in Personal Emergency Response System" published in Design and Diagnostics of Electronic Circuits & Systems (DDECS), 2015 IEEE 18th International Symposium.

[7] Iftekhar Uddin Ahmed, Nazia Hassan, Humayun Rashid,"Solar powered smart wearable health monitoring and tracking device based on GPS and GSM technology for children with autism", in 4th International Conference on Advances in Electrical Engineering (ICAEE),2017.

[8] R.Kumar and Dr.M.Pallikonda Rajasekaran "Raspberry PI based patient Health Status Observing Method Using Internet Of Things" Published in International Conference on Current Research in Engineering Science and Technology 2016.

[9] Omar S. Alwan, K. Prahald Rao, "Dedicated real-time monitoring system for health care using ZigBee", Electrical and Computer Engineering Department, Faculty of Engineering, King Abdulaziz University, Jeddah-21589, Saudi Arabi.

[10] Shashikant Ghumbre, Chetan Patil, and Ashok Ghatol "Heart Disease Diagnosis using Support Vector Machine" published in International Conference on Computer Science and Information Technology (ICCSIT'2011)

[11] Y. Shi, S. Abhilash, and K. Hwang, "Cloudlet mesh for securing mobile clouds from intrusions and network attacks," in *The Third IEEE International Conference on Mobile Cloud Computing, Services, and Engineering,(Mobile Cloud 2015)*. IEEE, 2015.

[12] J. Sun, F. Wang, J. Hu, and S. Edabollahi, "Supervised patient similarity measure of heterogeneous patient records," *ACM SIGKDD Explorations Newsletter*, vol. 14, no. 1, pp. 16–24, 2012.

[13] Thwe Thwe Ngwea, Su Wai Phyo "Digital Envelope System Based on Optimized NTRU (Number Theory Research Unit) and RC6 Algorithm" published in International Journal of Computer (IJC) (2015) Volume 19, No 1, pp 67-78.

[14] Y. Wu, M. Su, W. Zheng, K. Hwang, and A. Y. Zomaya, "Associative bigdata sharing in community clouds: The meepo approach," *IEEE CloudComputing*, vol. 2, no. 6, pp. 64–73, 2017.

[15] Wan-Young Chung,Young-Dong Lee, Sang-Joong Jung, "A wireless sensor network compatible wearable u-healthcare monitoring system using integrated ECG, accelerometer and SpO2", 30th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, 2008.

[16] Yong Lin, Xingjia Lut, Fang Fang and lianbo Fan "Personal Health Care Monitoring and Emergency Response Mechanisms" published in Future Information and Communication Technologies For Ubiquitous HealthCare Future Information and Communication Technologies for Ubiquitous HealthCare on 2014.

[17] J.-J. Yang, J. Li, J. Mulder, Y. Wang, S. Chen, H. Wu, Q. Wang, and H. Pan, "Emerging information technologies for enhanced healthcare, Computers in Industry, vol. 69, pp. 3–11, 2015.

[18] J.-J. Yang, J.-Q. Li, and Y. Niu, "A hybrid solution for privacy preserving medical data sharing in the cloud environment" published in Future Generation Computer Systems, vol. 43, pp. 74–86, 2015.