DATA SECURITY APPROACH IN IOT ENVIRONMENT

Shruti Sawardekar
Department of Computer Engineering
Sardar Patel Institute of Technology
Andheri, India
shruti.sawardekar@spit.ac.in

Renuka Pawar
Department of Information Technology
Sardar Patel Institute of Technology
Andheri, India
renuka_pawar@spit.ac.in

***Abstract*— The growth of internet has introduced different types of services which includes actuators and sensors proving remarkable and outstanding performances. It is found that the greatest current issue in IoT field is to obtain an easy and a safe access control scheme for the large amount of data. So there is a need to discover some solutions of security. This study discusses about the open API service which is a web service called as the IoT Thingspeak platform. It plays as a host for a different numbers of sensors for sensing and monitoring patients heart rate and temperature data at cloud level and further the data is being ported to MATLAB R2017a with the help of a channel ID. In MATLAB R2017a security is being applied to the patients data using GUI login details. The proposed technique is used for retrieving data securely at the end user. This work makes use of hardware components such as Arduino UNO board, ESP8266 Wi-Fi Module, Pulse sensor, LM35 Temperature sensor for processing and transferring the sensed information to the Thingspeak cloud.**

Keywords*— *Arduino ESP8266, Channel ID, Arduino UNO, Matlab R2017a, API Key, Thingspeak IoT cloud, Pulse senor, LM35 Temperature senor.

I. INTRODUCTION

The Internet of Things (IoT) is an encouraging model that integrates several communication and technical solutions. The IoT is defined as a field in which each physical object is to be connected at anytime and at any place with the help of internet and to be able in identifying these devices to other devices [1]. In the current era there have been remarkable advances in the field of IoT. According to a survey which estimated that there is an increase in connected devices over the years and the results are surprising. It is listed in the table as follows.

YEAR	NUMBER OF CONNECTED DEVICES
1990	0.3 million
1999	90.0 million
2010	5.0 billion
2013	9.0 billion
2025	1.0 trillion

Fig. 1. Rise in the number of connected devices

In the recent days, as information technology is developing, it is making rapid improvements in the branch of medical study. Taking into consideration the improvement in medical research, large amounts of medical data needs to be managed transparently and cost-effectively [5]. There are a lot many IoT applications and within those health care system is considered as one of the most significant challenges in the present world. With the rapid improvement in the field of medical research, there are new emerging technologies to help work faster with large amounts of data. Such data includes patient's medical records, treatment factors and diagnosis having security risks associated with it [10].

A. Arduino UNO board: Data processing board

Arduino UNO encompasses 'ATmega328' consisting of serial communication. Internally it consists of a Boot loader assisting in loading of Arduino programs. The language for programming used here is Arduino coding meaning APL that proposes wiring and Arduino Development environment i.e., ADE proposing processing. A user is required to connect microcontroller to the computer using a USB cable or a battery power. It as shown in the fig.

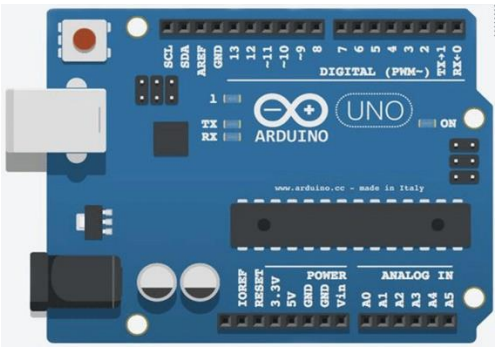

Fig. 2. Arduino UNO Board

B. Thingspeak: An IoT platform

Thingspeak is based on the internet or web which acts as a platform for providing information relating to IoT. It is a comprehensive platform source that stores sensor related data of a variety of applications coming under IoT. It then combines the data that is being sensed in graphical formats at the web level for analysis and visualization purposes. In Thingspeak platform, the communication process is carried out by internet connection

acting as packet of data that is a carrier between the components that are the things being connected.

C. Arduino ESP8266: Wi-Fi Module

Arduino ESP8266 is used for providing self-reliable and absolute Wi-Fi resolution of networking. The ESP8266 Wi-Fi module is preprogrammed itself with the AT command firmware set. It is being used widely for the IoT based applications which are embedded. It has a 2.4 GHz Wi-Fi. It has analog to digital conversion. It is as shown in the fig.

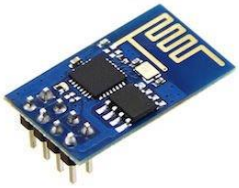

Fig. 3. Arduino ESP8266: Wi-Fi Module

II. Sensors Description

A. Pulse sensor

Pulse sensor is a properly designed sensor that is used by Arduino. Students, athletes, artists, and mobile game developers can make use of it for generating live blood pressure data and heart rate data in their projects. It can also be used by an open source app that continuously monitors data for generating graphs in real time. It is as shown in fig.

Fig. 4. Pulse Sensor

B. LM35 Temperature Sensor

LM35 is a temperature sensor. The temperature measured using this LM35 temperature senor is more accurate than that measured with a thermistor. The range in which it operates is -55 degree Celsius to 150 degree Celsius.

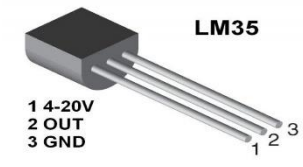

Fig. 5. LM35 Temperature Sensor

C. Motivation

As the field of IoT in healthcare is improving rapidly, there arises need to manage the health records properly and provide efficient treatment to patients. The motivation behind this research work is to properly secure patients data without leaking it by integrating hardware and software components. This paper talks about securing data of patients as well as additionally it includes accessing of patients data by patients and doctor at any time and at any place which is being proposed in this work.

III. Relation to Prior Work

(AAL) framework is designed which is one among the huge applications in internet of things. It is an environment related to home elevated with ambient sensors embedded in it in order to improve one's quality of life. The main aim of this framework is to focus the challenges and issues so as to provide security and safety while accessing sensitive health data [1]. On the basis of smartphone monitoring of pressure of blood pressure application is developed and evaluated. The technique developed is based on the measurement of the time when the valve of aortic opens and pulse after arriving a particular site of arterial [2]. The proposed system integrates devices of IoT in a system of control of access that is being developed for services on basis of web by designing some internet of things communication components. With the help of this, unique technique of controlling of access can be obtained among different devices.

The convenient protocols for communication are analyzed for the scenario and a methodology is being proposed that permits designing of actions of communications of resources [3]. A novel access control architecture is being proposed for improving management of policy authentication in a huge system of health care by decreasing the number of policies by giving access control of fine grained manner [4]. The sensitive data is secured by encryption for the purpose of transmission and it also provided with the prevention of security attacks and threats and also for secured transmission [5]. A security is provided as well as smart technique for storing information related to health is being designed using advanced security mechanisms and machine learning for handling big data of medical industry [6].

A system for monitoring health of patients in IoT is designed with the help of Arduino to study parameters and data collected using sensors [7]. The light weight network of body sensing is proposed for finding the weaknesses that are studied in previous techniques of IoT in healthcare [8]. The proposed system mainly focuses on securing health care personal data by making use of a fog computing facility in a cloud environment [9]. The various security requirements are analyzed that are being used in a number of different health care system [10]. It proposes a smart gateway that provides protection to the entire system by making use of changed protocol of identity of host for exchange of diet (HIP-DEX) which is a protocol for exchange of key [11].

ECC algorithm is used for securing the information of patients by developing a system that incorporates this facility [12].

Comparative analysis is done for various IoT techniques used in a Health care system. The different methods are being studied that discuses about the health care issues in the field of IoT [13]. Security model of Context aware access control is designed that is on basis interoperability of data [14]. The proposed work is based on the comparison of AES as well as MASK algorithm. Both the algorithms are compared using diffusion, confusion terms [15]. In the proposed system, the protocol of authorization of web (OAuth) is used combing accompanied by the user managed access (UMA) [16]. The security requirements are being examined of extended RBAC security model and privacy protection. A service platform for RBAC based personalizing health care is developed for the purpose of managing smartly the records of health using well developed devices [17]. An efficient and management of key in secure manner is proposed on basis of ECC algorithm for protecting medical data of patients in health care environment [18].

A system is developed that protects privacy of patients and their data by non removal of sensitive attributes. From the findings it is noticed that with the help of implemented technique, the statistics and properties of the level of dataset are found to be proper even later performing masking of data [19]. The architecture is proposed that can be uniformly used across in the industry part for the purpose of testing data that are critical in terms of business [20].

IV. Softwares Used

A. *Arduino IDE Software*

The Arduino IDE is a development software that is integrated and used for Arduino device. It helps the Arduino microcontrollers in coding for interfacing of the sensors and also some other components. It makes use of library functions for performing operation on both local and global domain.

B. *Matlab R2017a*

The Matlab R2017a acts as an opportunity for providing reliability for IoT based projects. In the present era, Thingspeak is the only IoT web service which is offering data analysis on the Matlab platform. Full profile access is available on Matlab and analyzing can be done as per the requirement of project.

V. Proposed Model and Hardware Setup

Description of proposed system - Handling large amounts of medical records of patient can be a difficult task for the large organizations. Also these sensitive information can be leaked and manipulated for various illegal and promotional purposes by the malicious users. So there is a need that the sensitive information should be properly managed and controlled by the patient as well as trusted entities in order to avoid such circumstances. As well as patient and other assigned authorities should be able to give authority to other users of the organization so that the patients may not face any issues in their treatment even in future when they are not the part of the particular organization. Also it will be helpful in future to other patients who needs to use the approach to keep themselves secure. Using data masking technique the sensitive data needs to masked appropriately as well as UMA approach needs to be designed in such a way that allows proper defined user access and overcome the existing security attacks by finally presenting the resulted outcomes by performing data visualization and analysis.

The overall process is carried out in following manner.

Phase I-

Step.1 - Loading of sensor libraries into the Arduino IDE Software.

Step.2 - Executing the program and visualizing sensed data displayed on serial monitor.

Step.3 - Network credentials to be entered in IDE and executing the program once again and finally visualizing the output obtained in Thingspeak cloud.

The sensing monitoring system process based on Thingspeak for IoT is as shown in flowchart below.

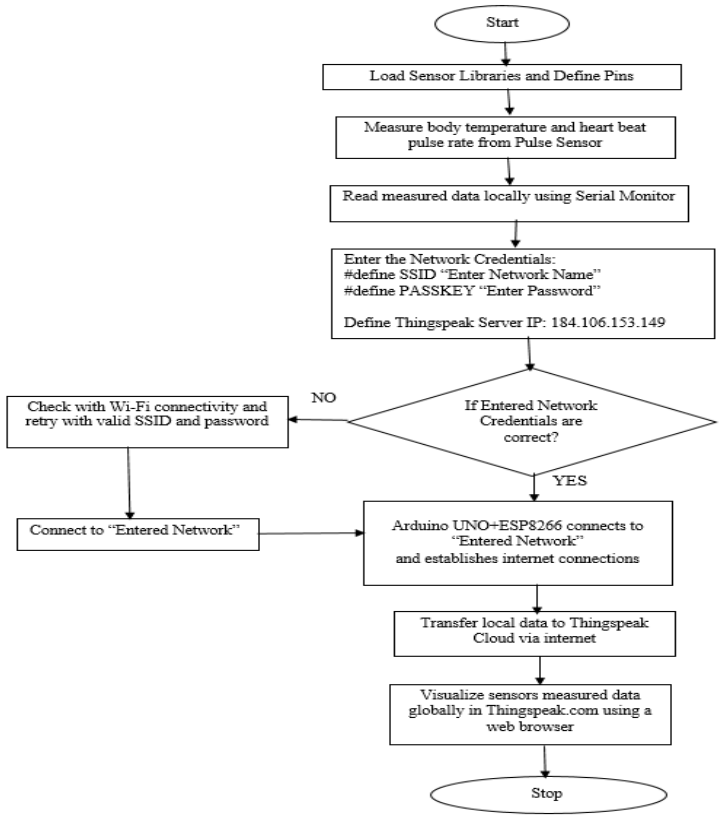

Fig. 6. Thingspeak Based Sensing Monitoring System Process Flowchart for Iot

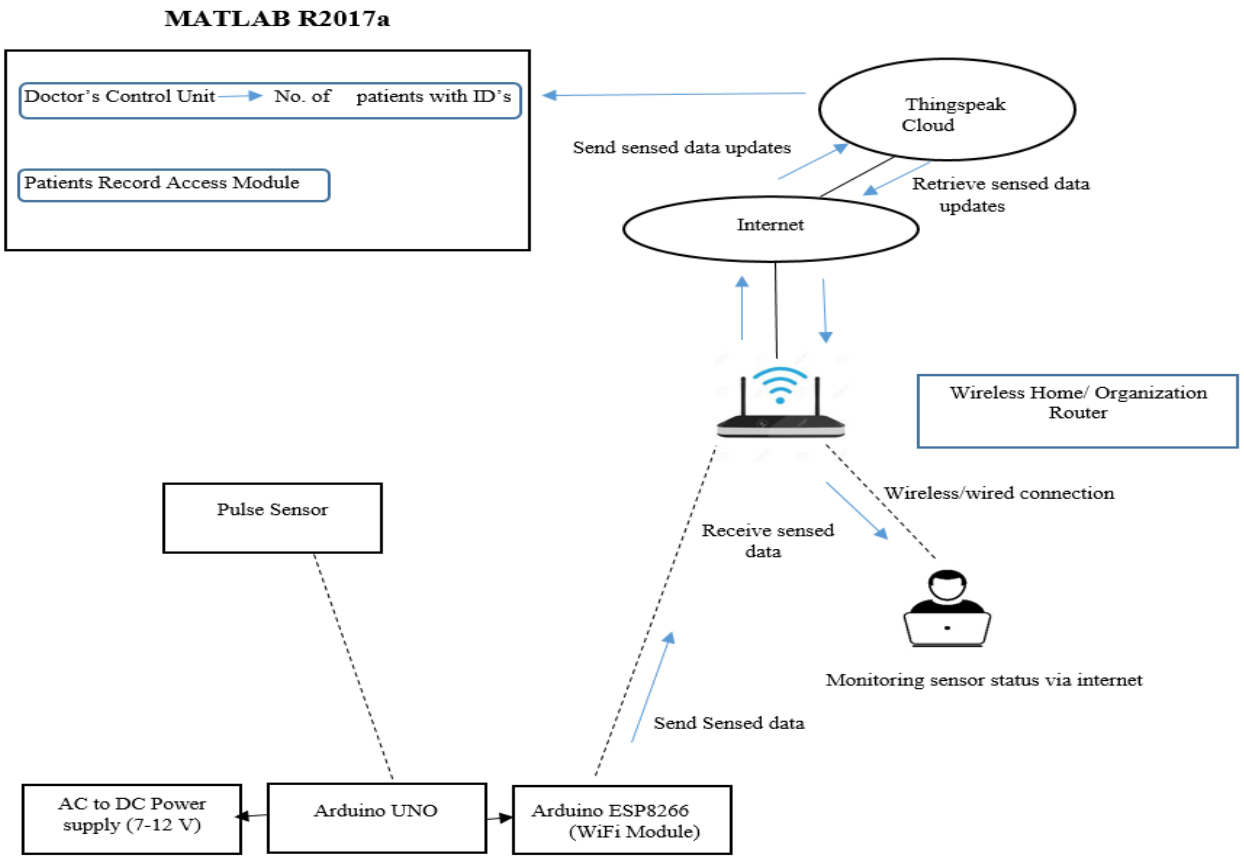

Fig. 7. Proposed System

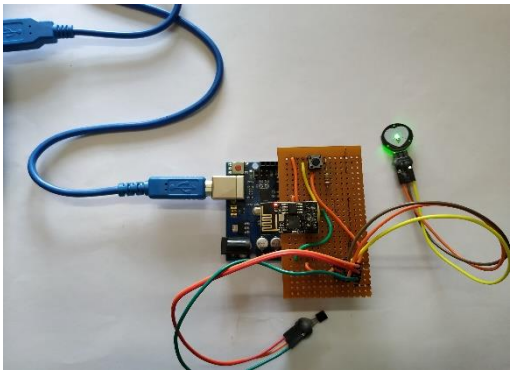

Fig. 8. Hardware Setup

Phase II- The data analysis in the Matlab R2017a is carried out in Thingspeak. Data visualization is carried again in Thingspeak. Later the sensed data needs to be analyzed in the Matlab R2017a. For the same purpose Thingspeak supporting toolbox is essential. It helps in porting of the data that is sensed from Thingspeak cloud. Coding is done using the Matlab platform after the installation of the toolbox. In order to successfully extract data from the cloud we use the channel ID for the reading and collecting of data purpose.

Step.1- Enter the Channel ID as to read Channel ID.

Step.2- Execute the code written in Matlab. The code will read the channel ID. The data sensed in the Matlab is further ported into the Matlab R2017a in the form of graphs and it is being discussed in the following results and discussion section.

Phase III- On obtaining the Channel ID the IoT sensed data can be used for analysis and carrying out the further operations. Graphical User Interface is created for the exchange of data and its analysis. In this login details are created for patients and doctors. Kd tree data masking algorithm is being applied on the data sensed from Thingspeak to calculate the nearest neighbors. On this value encryption and decryption is being applied. Doctors can access patients data and patients can even view their data. Login details are created for both the patients and doctor. After enter the login ID doctor can access heart rate and temperature of patients. The heart rate plot and temperature plot shows the original, encrypted and decrypted plots.

VI. Results and Discussions

This section shows the output in the graphical formats. They are as follows.

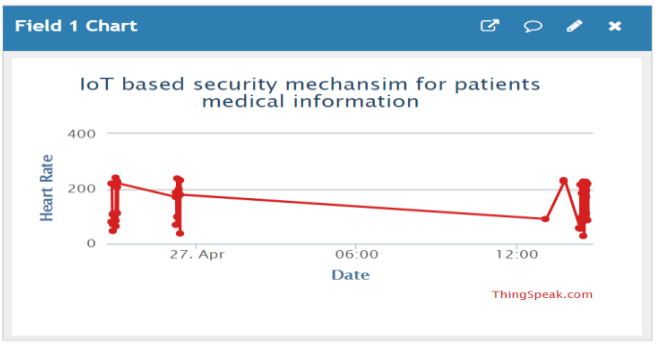

Fig. 9. Thingspeak Graph of Heart Rate

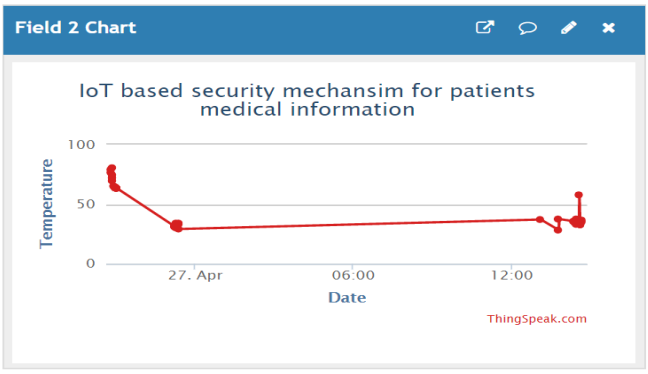

Fig. 10. Thingspeak Graph of Temperature

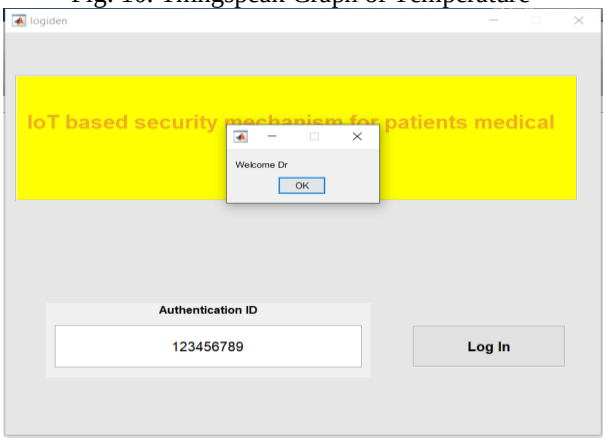

Fig. 11. Matlab Login Access Window of Doctor

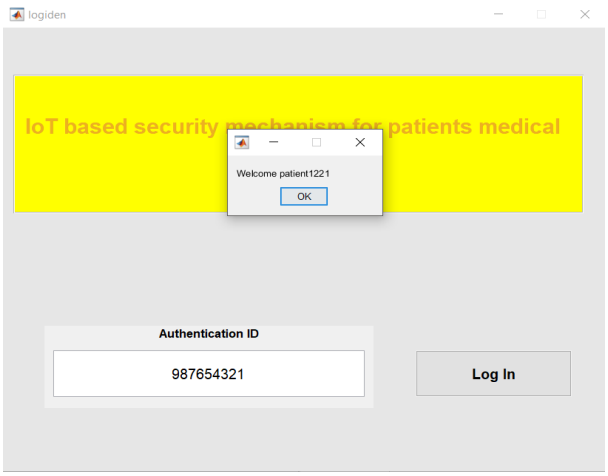

Fig. 12. Matlab Login Access Window of Patient

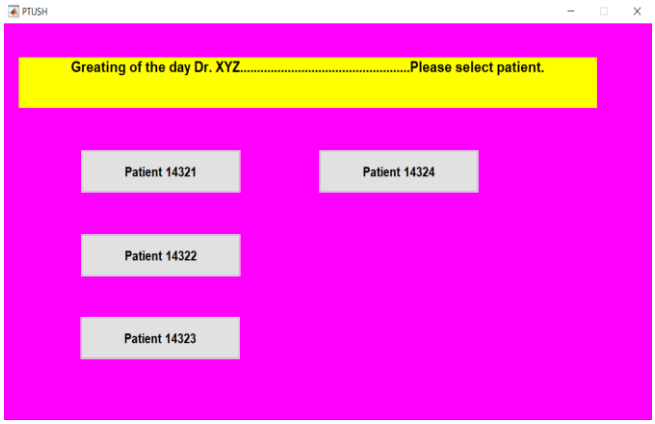

Fig. 13. Patient Selection

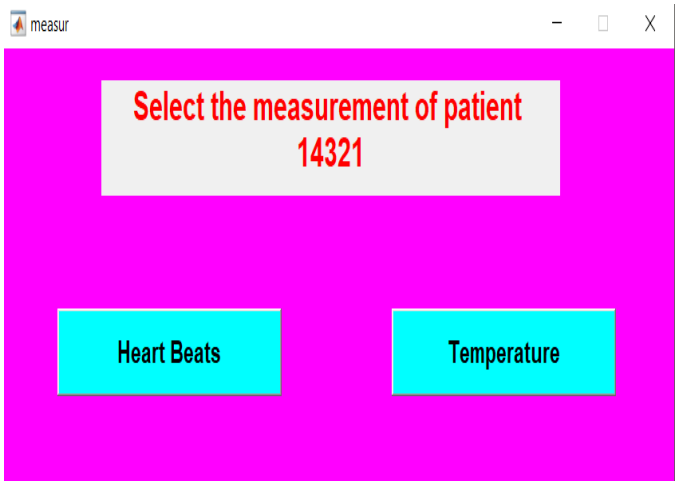

Fig. 14. Parameter Selection

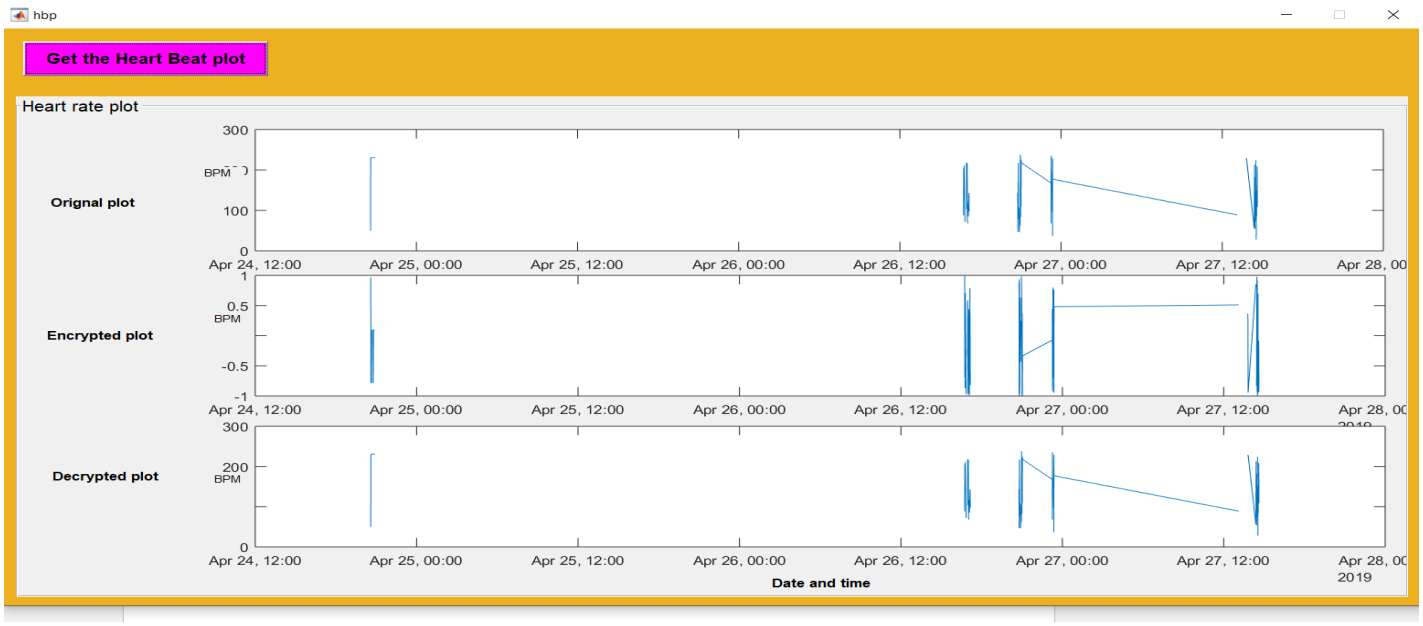

Fig. 15. Heart Beat Plot

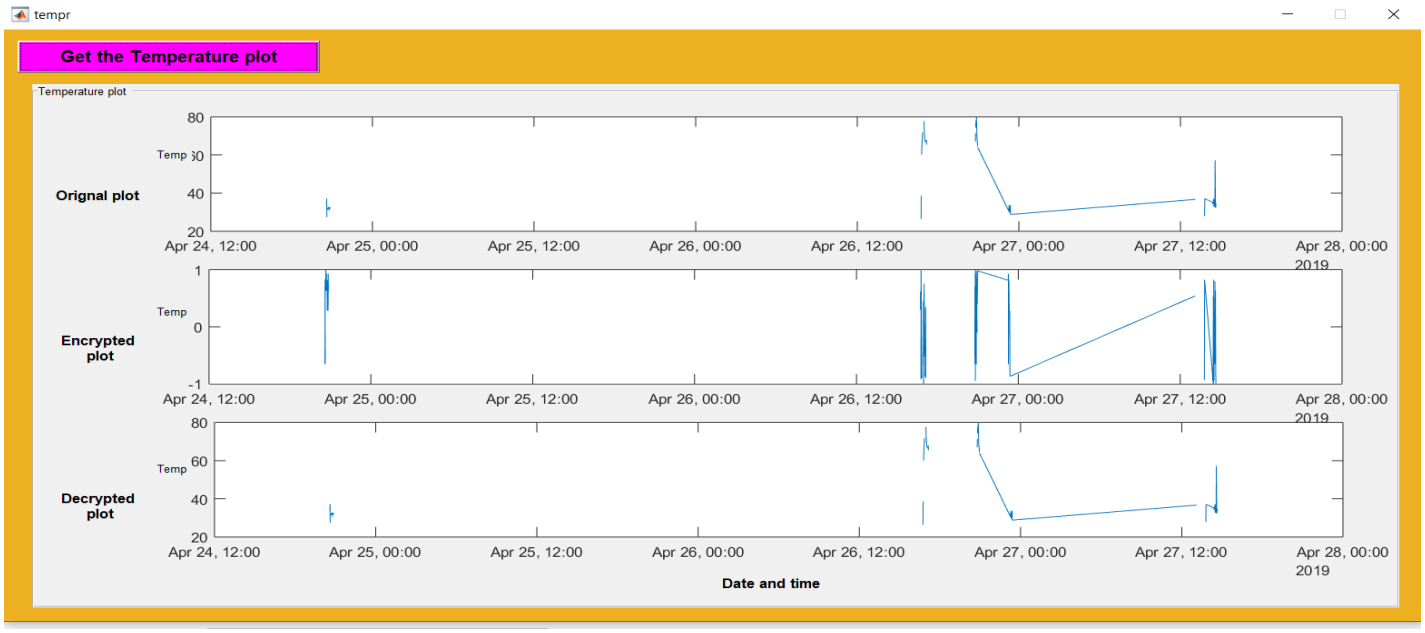

Fig. 16. Temperature Plot

VII. Conclusion & Future Work

The IoT in Health care is proving tremendous growth. It is remarkably increasing across different specific Internet of Things use cases. It is also observed that use cases of IoT are increasing tremendously as well as the reality connecting health care is moving rapidly although the obstacles exist. This paper discusses about IoT health care scenarios. The various techniques are addressed along with their limitations. Data masking technique is used here for protecting patient's medical information and a User Managed Access approach is designed for defining various rights of accessing the personal information. The limitation of this research work is that additional parameters of patients are not being discussed and proposed like blood pressure monitoring, respiration rate, ECG (Electrocardiogram).Inclusion of these parameters can help patients improve their health. In future work, the proposed technique can be improved for better results. It can be done on user side, when data is input data is being taken up. The data after encrypting can be transferred to the cloud.

REFERENCES

[1] Usama Salama, Lina Yao and Hye-young Paik, "An Internet of Things Based Multi-Level Privacy-Preserving Access Control for Smart Living", {Informatics (Basel), vol. 5, no. 23, 3 May 2018.

[2] Edward Jay Wang, Junyi Zhu1, Mohit Jain, Tien-Jui Lee, Elliot Saba, Lama Nachman, and Shwetak N.Patel , "Seismo: Blood Pressure Monitoring using Built-in Smartphone Accelerometer and Camera", Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, no. 425, April 2018.

[3] Cruz-Piris L, Rivera D, Marsa-Maestre I, de la Hoz E, and Velasco JR., "Access Control Mechanism for IoT Environments Based on Modelling Communication Procedures as Resources", Sensors (Basel) ,vol.18, no. 917, 20 March 2018.

[4] Shantanu Pal, Michael Hitchens, Vijay Varadharajan, and Tahiry Rabehaja, "Fine-Grained Access Control for Smart Healthcare Systems in the Internet of Things", EAI Endorsed Transactions on Industrial Networks and Intelligent Systems, vol. 4, no. 13, 20 March 2018.

[5] M.Prabhu, G.Seethalakshmi, and Gollapudi Anisha, "Secured Healthcare System in IoT", International Journal of Pure and Applied Mathematics, vol. 118, no. 20, 2018.

[6] Prableen Kaura, Manik Sharmab, and Mamta Mittalc, "Big Data and Machine Learning Based Secure Healthcare Framework", International Conference on Computational Intelligence and Data Science (ICCIDS 2018), no. 132, pp. 1049-1059, 2018.

[7] V.Akhila, Y.Vasavi, K.Nissie, and P.Venkat Rao, "An IoT based Patient Health Monitoring System using Arduino Uno", International Journal of Research in Information Technology, vol. 1, no. 1, pp. 1-9, November 2017.

[8] Yong-Yuan Deng, Chin-Ling Chen, Woei-Jiunn Tsaur, Yung-Wen Tang and Jung-Hsuan Chen, "Internet of Things (IoT) Based Design of a Secure and Lightweight Body Area Network (BAN) Healthcare System", Sensors (Basel), vol. 17, no. 12, 15 Dec 2017.

[9] Hadeal Abudulaziz Al Hamid, SK MD Mizanur Rahman , M. Shamim Hossain , Ahmad Almogren , and Atif Alamri, "A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility With Pairing-Based Cryptography", IEEE , vol. , pp. 22313-22328, 28 September 2017.

[10] Sejal Patel, Narendra Singh, and Sharnil Pandya , "IoT based Smart Hospital for Secure Healthcare System", International Journal on Recent and Innovation Trends in Computing and Communication , vol. 5, no. 5, pp. 404-408, May 2017.

[11] Binu P. K., Karun Thomas, and Nithin P. Varghese, "Highly Secure and Efficient Architectural Model for IoT Based Health Care Systems", International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 487-493, 2017.

[12] R.Sridevi, and C.Nithiya, "E-Health Security using ECC algorithm", International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST), vol. 2, no. 19, pp. 114-117, October 2016.

[13] Suriya Begum, and Venugopal, "Comparison of Various Techniques in IoT for Healthcare System", International Journal of Computer Science and Mobile Computing, vol.5, no. 3, pp. 59-66, March 2016.

[14] Isra Ahmed Zriqat and Ahmad Mousa Altamimi, "Security and Privacy Issues in Ehealthcare Systems: Towards Trusted Services", International Journal of Advanced Computer Science and Applications (IJACSA), vol. 7, no. 9, pp. 229-236, 2016.

[15] Heera G. Walia and Nalini C. Iyer, "Modified MASK Algorithm for Image Encryption", International Conference on Information Security & Privacy (ICISP2015), no. 78, pp. 603-609, December 2015.

[16] H. Tschofenig, E. Maler, E. Wahlstroem and S. Erdtman, "Authentication and Authorization for Constrained Environment Using OAuth and UMA", 2015.

[17] Moon Sun Shin, Heung Seok Jeon, Yong Wan Ju, Bum Ju Lee, and Seon-Phil Jeong, "Constructing RBAC Based Security Model in u-Healthcare Service Platform", The Scientific World Journal, 2015.

[18] Young sil Lee, Esko Alasaarela, and Hoon Jae Lee, "Secure Key management Scheme based on ECC algorithm for Patient's Medical Information in Healthcare System", IEEE International Conference on Information Networking , pp. 453-457, February 2014.

[19] Luvai Motiwalla and Xiao-Bai Li, "Developing privacy solutions for sharing and analysing healthcare data", International Journal of Business Information Systems, vol. 13, no. 2, pp. 199-216, 2013.

[20] G K, Ravikumar & Manjunath, TN & Hegadi, and Ravindra, "Design of Data Masking Architecture and Analysis of Data Masking Techniques for Testing", International Journal of Engineering Science, vol. 3, no. 6, pp. 5150-5159, June 2011.