Security In Healthcare Monitoring System

Chavan Jyoti
Under Graduate Student
Computer Department
JSPM's Rajarshi Shahu College of Engineering
Pune, India

Imade Tanuja
Under Graduate Student
Computer Department
JSPM's Rajarshi Shahu College of Engineering
Pune, India

Kalbhor Vaishnavi
Under Graduate Student
Computer Department
JSPM's Rajarshi Shahu College of Engineering
Pune, India

Kolawale Karishma
Under Graduate Student
Computer Department
JSPM's Rajarshi Shahu College of Engineering
Pune, India

ABSTRACT

Hospitals are necessary to constantly monitor the patient's physiological parameter. The technology plays an important role in healthcare not only for sensory devices but also in communication and display device. According to medical statistics death rate is increasing due to temperature and heartbeats of the patient. Hence the latest trend in healthcare communication using IOT is adapted. In this project, the microcontroller is used as a gateway to communicate to the various sensors such as a temperature sensor and heart rate sensor. The microcontroller picks up the sensor data and sends it to the server through Wi-Fi and hence provides real-time monitoring of the health care parameters for doctors. The data can be accessed anytime and from anywhere by the doctor. The microcontroller is connected to the buzzer which monitors variation in temperature and heartbeats. If the value of this parameter crosses the threshold alert is given to the doctor and the patient's relative through the buzzer. But the major issue in the patient monitoring system is that the data has to be securely transmitted to the system and provision is made to allow only authorized user to access the patient data. The security issue is been addressed by transmitting the data through the password protected Wi-Fi module which will be encrypted by the standard AES algorithm and the doctor can access the data by logging to the webpage. At the time of emergency situation alert message is sent to the ambulance through the GSM module connected to the controller with the patient location. Hence quick action can be easily done by this system. This system has features like low power consumption capability, easy setup, high performance and time to time response and user-friendly GUI.

Keywords—IOT, Security, Healthcare, Cloud, Secure Sharing of Personal Healthcare Records(SeSPHR)

I. INTRODUCTION

A healthcare system should give better healthcare services to people anywhere in an affordable and patient comfortably manner. Recently, the healthcare system is going to change from an old approach to a new patient-centered approach[1]. To check a patient's diagnosis and advising doctor need to visit the patients. The two basic problems related to this approach, very first the doctors compulsory should present at the place of the patient for 24 hours. The second problem is in the hospital, the patient remains admitted, a wiring connected biomedical instruments to the bedside, for a long period of time. The patient-friendly approach has received to solve these two problems. In this system, the patients are aware of knowledge and information to play a more active role in disease diagnosis, and prevention. The important element of this second approach is reliable and readily available patient monitoring system (PMS)[2]. Healthcare is the challenging field for many software developers in the world. According to the compositions of the World Health Organization (WHO), the highest achievable standard of health is an important right for a single[3]. Health is wealth. Healthy persons can also reduce pressure on the already overloaded hospitals, clinics, and medical professionals and decrease the workload on the public safety charities, governmental or non-governmental centers, and networks. To a human being healthy, a readily easy going modern healthcare system is essential.

Smart applications can be designed that can present sustainable medical interventions efficiently at low cost in a user-friendly manner[4]. According to the World Health Organization (WHO), the death rate due to heart disease is increasing across the world[5]. Heartbeats are a crucial risk factor for ischemic heart diseases and thus, preventive measures must be taken against it. The proposed system aims to monitor the patient's

heartbeats and temperature. As the uses of IoT devices are increasing the issues related to security and risk is also increasing[6]. Proposed system aims to provide the security to patient healthcare data collected by sensors and reports uploaded by patients and doctors. For providing security system is using AES (Advanced Encryption Standards) algorithm[7][8].

Data dropout was a significant challenge, mainly due to infrastructure problems (interruptions in the hospital Wi-Fi service) or expired batteries. The ECG sensor had the bare minimum battery life required for use on the ward (at approximately 24 h) such that nurses could change the device once per day. Shorter battery life would require several changes per day, which is deemed unrealistic for clinical practice. The actual quantity of data ultimately collected was large. The proposed system solves the above problems using this problem by developing a smart application with the alert[9]. The system helps the doctor to monitor the patient at any time and anywhere. Security to patient data was another major challenge in healthcare. The proposed system monitors the data transmission between patient and doctor and provides secure patient healthcare system[10][11].

This paper is organized as follows. Section 2 discusses the existing methodologies on the healthcare monitoring system. The proposed methodology is presented in section 3 whereas section 4 concludes the paper.

II. RELATED WORK

In this section, the existing works that relate to the proposed work are presented. The author in [12] suggested the system that provides an inexpensive and efficient IOT[13] based application for healthcare monitoring and tracking that can help in taking care of the patient's health. This system will thus be beneficial for both the patient and the doctor in case of medical emergencies. The authors in [14] explained a methodology of Secure Sharing of Personal Healthcare Records (PHRs) in the cloud. The methodology preserves the confidentiality of the PHRs and enforces patient-centric access control to different portions of the PHRs based on the access provided by the patients. We implemented a fine-grained access control method in such a way that even the valid system users cannot access those portions of the PHR for which they are not authorized. The PHR owners store the encrypted data on the cloud and only the authorized users possessing valid re-encryption keys issued by a semi-trusted proxy are able to decrypt the PHRs.[15] Analyzed the resource utilization of AES Encryption on IoT devices. This paper serves to provide an in-depth analysis of three different implementations of AES on two different IoT boards with respect to their energy and encryption duration across available key sizes and buffer sizes. Security algorithms must share resources with other computational work or I/O, so it is imperative that these algorithms be efficient to minimize the overall cost of security such that they can be effectively used alongside other functionality.

The authors in [16] suggested the system to design an IOT based smart healthcare system using an Arduino microcontroller. In this work, the Pulse oximeter is designed and the DS1820B temperature sensor is used to read the temperature and heart rate of the patient and the microcontroller picks up the data. This data is sent to cloud it through the Arduino Wi-Fi module. The patient can access this data. In emergency conditions, the alert message is sent to the doctor's cell phone through the GSM modem connected[17]. The doctors can view the sent data by login into the system by unique login ID. Hence continuous patient monitoring system is designed.[18] Explained that a mobile physiological monitoring system, which is able to continuously monitor the patient's heartbeat, blood pressure and other critical parameters in the hospital. The system is a combination of a coordinator node to acquire the patient's physiological data, a WMHRN to forward the data and a BS to collect the data. The system is able to carry out long-term monitoring on patient's condition and is equipped with an emergency rescue mechanism using SMS/E-mail. [19] Suggested that based on IOT functional principles and design it allows direct communication of the sensor devices with the cloud application.[20] Proposes a novel cooperative IoT approach for rural healthcare applications like safe motherhood program and many more. This paper explained the application of IOT in the healthcare field. IOT has various applications in the field of healthcare domain which helps patient and doctor to save time and effective use of the system.

III. PROPOSED SYSTEM

The proposed system is as follows

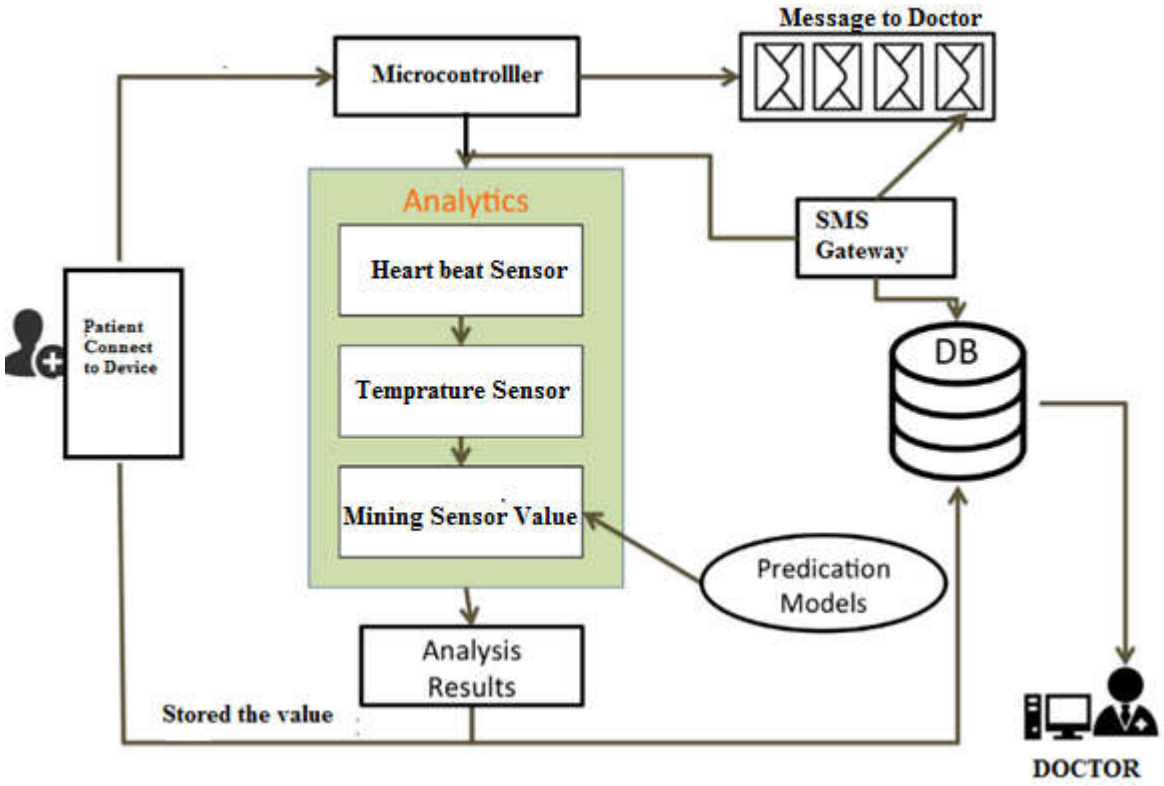

Fig.1 System Architecture

The main idea of the designed system is to continuous monitoring of the patients over the internet. The Proposed System architecture for IOT Healthcare is as shown in the Figure. The model consists of Arduino (ESP8266) Microcontroller, a Temperature sensor (DS18B20), Pulse Oximeter Sensor (TCRT1000), GSM MODEM, Piezo Electric Buzzer, Wi-Fi Module, GSM Modem, and Regulated Power Supply. In this system, ESP8266 Microcontroller collects the data from the sensors and sends the data through Wi-Fi Protocol. The Protected data sent can be accessed anytime by the doctors by typing the corresponding unique IP address in any of the Internet Browser at the end user device(ex: Laptop, Desktop, Tablet, Mobile phone). The Microcontroller is connected to GSM Modem which provides information to doctor and patient relatives when the heart rate is greater than 90 or less than 60 and when the temperature is less than 20 or greater than 35. During this time the buzzer turns on and alerts the caretaker. LCD is connected to the microcontroller to display the transaction process and healthcare data. And the user interfaces HTML webpage will automatically refresh for every 15 seconds hence patient health status is continuously sent to the doctor. Hence continuous monitoring of patient data is achieved.

After patient data is sent to cloud the transmission of data between doctors and patient is secured by using AES encryption and decryption algorithm[21][22]. The performance of the system methodology to securely share patient healthcare records among different types of users are evaluated by developing a client application in Java. The proposed system uses Embedded C Programming for hardware interface. The entities of the proposed system methodology include the cloud and the users. We are using Amazon Simple Storage Services (Amazon S3)[23] as our cloud storage. Advanced Encryption Standard is used for the encryption of PHR data. The experiments will conduct on the computer having Intel(R) Core i3-4005U CPU @ 1.70 GHz with 4 GB memory.

IV. CONCLUSION AND FUTURE SCOPE

The proposed system is more efficient and beneficial. It uses low cost, a lightweight sensor which monitors the patient continuously and proper messages are provided in an emergency. Thus it saves the life of a patient when abnormal conditions take place. A dynamic integration related to multimedia medical data provides the framework which is low overhead and rich multimedia support. The wireless medium develops a wireless emergency healthcare system for an environment that integrates with several technologies such as Microcontroller, Sensors, and SMS. The system provides security to the patient's data.

Future Scope:

This project can be further improved by including,

- ECG Blood pressure.
- The nearest hospital will be informed automatically with the help of GPS and ambulance will be sent to the patient.
- Automatically calling the doctor in case of emergency.

V. ACKNOWLEDGMENTS

I wish to express my profound thanks to all who helped us directly or indirectly in making this paper. Finally, I wish to thank all our friends and well-wishers who supported us in completing this paper successfully I am especially grateful to our guide Prof. S. B. Javheri for time to time, very much needed, valuable guidance. Without the full support and cheerful encouragement of my guide, the paper would not have been completed on time.

REFERENCES

[1] Mohyuddin, W. A. Gray, H. Bailey, C. Jordan, and D. Morrey, "Wireless patient information provision and sharing at the point of care using a virtual organization framework in clinical work," *6th Annu. IEEE Int. Conf. Pervasive Comput. Commun. PerCom 2008*, pp. 710–714, 2008.

[2] B. Srimathi and T. Ananth, "A Review on Patient Healthcare Monitoring," vol. 6, no. Xi, pp. 96–101, 2018.

[3] S. W. A. Gunn, "The right to health," *Concepts Pract. Humanit. Med.*, no. 31, pp. 3–7, 2008.

[4] K. K. Reddy, P. lalit. S. Reddy, and D. P. B. Reddy, "Study on Mobile Healthcare System," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 4, no. 3, pp. 143–148, 2014.

[5] "The top 10 causes of death." [Online]. Available: https://www.who.int/news-room/fact-sheets/detail/the-top-10-causes-of-death. [Accessed: 28-Dec-2018].

[6] H. K. Patil and R. Seshadri, "Big data security and privacy issues in healthcare," *Proc. - 2014 IEEE Int. Congr. Big Data, BigData Congr. 2014*, pp. 762–765, 2014.

[7] R. Borhan, "Successful Implementation of AES Algorithm in Hardware," pp. 27–32, 2012.

[8] M. Khader, M. Alian, and S. Almajali, "Applications on the Internet of Thing," 2017.

[9] M. Shelar, "Wireless Patient Health Monitoring System," vol. 62, no. 6, pp. 2–6, 2013.

[10] J. Shen, T. Zhou, X. Chen, J. Li, and W. Susilo, "Anonymous and Traceable Group Data Sharing in Cloud Computing," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 4, pp. 912–925, 2018.

[11] H. Tao, M. Z. A. Bhuiyan, A. N. Abdalla, M. M. Hassan, J. M. Zain, and T. Hayajneh, "Secured Data Collection with Hardware-based Ciphers for IoT-based Healthcare," *IEEE Internet Things J.*, vol. PP, no. X, p. 1, 2018.

[12] S. Bag and A. Bhowmick, "Smart Healthcare Monitoring and Tracking System," pp. 3085–3088, 2017.

[13] H. Huang, T. Gong, N. Ye, R. Wang, and Y. Dou, "Private and Secured Medical Data Transmission and Analysis for Wireless Sensing Healthcare System," *IEEE Trans. Ind. Informatics*, vol. 13, no. 3, pp. 1227–1237, 2017.

[14] M. Ali, A. Abbas, U. Khan, and S. U. Khan, "SeSPHR: A Methodology for Secure Sharing of Personal Health Records in the Cloud," *IEEE Trans. Cloud Comput.*, vol. PP, no. c, pp. 1–1, 2018.

[15] P. S. Munoz, N. Tran, B. Craig, B. Dezfouli, and Y. Liu, "Analyzing the Resource Utilization of AES Encryption on IoT Devices," no. November, pp. 1200–1207, 2018.

[16] D. A, K. Keerthana, N. Kiruthikanjali, G. Nandhini, and G. Yuvaraj, "Secured Smart Healthcare Monitoring System Based on IOT," *Ssrn*, pp. 4958–4961, 2017.

[17] P. A. Laplante, M. Kassab, N. L. Laplante, and J. M. Voas, "Building caring healthcare systems in the Internet of Things," *IEEE Syst. J.*, vol. 12, no. 3, pp. 3030–3037, 2018.

[18] M. Aminian, "A Hospital Healthcare Monitoring System Using Wireless Sensor Networks," *J. Heal. Med. Informatics*, vol. 04, no. 02, pp. 4–9, 2013.

[19] C. Doukas and I. Maglogiannis, "Bringing IoT and cloud computing towards pervasive healthcare," *Proc. - 6th Int. Conf. Innov. Mob. Internet Serv. Ubiquitous Comput. IMIS 2012*, pp. 922–926, 2012.

[20] V. M. Rohokale, N. R. Prasad, and R. Prasad, "A cooperative Internet of Things (IoT) for rural healthcare monitoring and control," *2011 2nd Int. Conf. Wirel. Commun. Veh. Technol. Inf. Theory Aerosp. Electron. Syst. Technol. Wirel. VITAE 2011*, no. April 2011.

[21] L. Zhu, Y. Wang, and R. Li, "Efficient Differential Fault Analysis Attacks to AES Decryption for Low-Cost Sensors in IoTs," no. 61173036, pp. 554–557, 2016.

[22] Y. F. Shen, "The implementation of the anti-attack AES mathematical model in library network encryption," *3rd Int. Conf. Mater. Sci. Inf. Technol. MSIT 2013*, vol. 756–759, no. Iccia, pp. 2944–2947, 2013.

[23] H. Abdulaziz *et al.*, "A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility with Pairing-Based Cryptography," vol. 3536, no. XX, pp. 1–17, 2017.