DEVELOPMENT OF IOT BASED SMART REAL TIME HEALTH CARE MONITOR

Imdhath G M, Project Developer, IOT Arena, Cuddalore, India, imdhath12311@gmail.com

Wasim G M, II Year B.Tech IOT, School of Computer Science & Technology, Faculty of Engineering & Technology, Jain University, Bangalore, India, wasim.imdhath@gmail.com

Abstract: *The multifaceted nature of the challenge demands a comprehensive approach that encompasses encryption, authentication, network segmentation, and ongoing vigilance in medical data analysis and processing. Implementing strong encryption protocols, robust authentication mechanisms, and network segmentation helps create a resilient defense against unauthorized access. Regular updates, both in terms of software and firmware, are essential to address emerging vulnerabilities. Physical security measures, data integrity validation, and privacy*

protection mechanisms contribute to a holistic security posture. Ultimately, by integrating these best practices into the design, deployment, and maintenance of wireless transmission systems for medical IoT devices, healthcare organizations can foster a secure environment conducive to the advancement of personalized healthcare while prioritizing patient trust and confidentiality. Regular reassessment and adaptation to evolving security challenges will be crucial in upholding the integrity of medical data transmission and sustaining the benefits of personalized healthcare IoT. This paper aims at bringing a new protocol to ensure the safety measures in the medical data analysis using IOT.

1. INTRODUCTION

Addresses the transformative impact of cutting-edge technologies on healthcare is the most important challenge in today's technology. By incorporating devices for continuous health monitoring, automated therapies, and real- time data tracking, it aims to revolutionize illness prevention and management. Leveraging high-speed internet and smartphones, particularly among the elderly, these technologies are seamlessly integrated into telemedicine via the Internet of Things (IoT). The paper's focal point is the development of an IoT-sensor-based monitoring system designed for real-time tracking of vital parameters, catering specifically to the needs of elders and children. This system not only facilitates in- home monitoring but also allows low-cost, real-time data transmission to remote physicians. medical data, compliance with the Health Insurance Portability and Accountability Act (HIPAA) is essential. The strict application of security measures, such as data encryption, access limits, and audit trails, is required in order to comply with HIPAA standards.

The idea is to use cutting-edge encryption methods to protect medical data while it is sent wirelessly between locations. The data is encoded using encryption algorithms, including Advanced Encryption Standard (AES), which prevents any unauthorized parties from deciphering it when they try to intercept or access it. During the data transmission process, authentication measures are essential for confirming the identities of the sender and the recipient. Robust authentication techniques, including biometric authentication or digital certificates, aid in verifying the identity of people accessing or sending data via wireless networks. This lowers the possibility of unauthorized access or data breaches by guaranteeing that only authorized people or devices with the right credentials can access and interact with the medical data. Introducing secure communication methods into place is crucial to protecting medical data while it's being transmitted wirelessly. Encryption and authentication are provided by protocols such as HTTPS (HTTP over SSL/TLS) and MQTT with TLS, which guarantee data integrity and secrecy during transmission. By creating secure channels of communication between devices Securing wireless data transmission in healthcare environments requires extensive security mechanisms including firewalls, intrusion detection/prevention systems (IDS/IPS), and frequent security audits in addition to encryption and authentication. Network traffic is monitored by firewalls and IDS/IPS systems for any unusual behavior or unauthorized access attempts. Security audits assist in locating and resolving possible vulnerabilities in the wireless infrastructure. In general, the objective of protecting wireless data transfer of medical information for customized healthcare is to take advantage of technology breakthroughs while giving patients' privacy and confidentiality first priority. Healthcare providers can provide individualized healthcare services with confidence and trust by putting strong security measures and processes in place to guarantee that patient data is safeguarded throughout its travels across wireless networks.

2. MOTIVATION:

Targeting the elderly and children, it aims to develop a cost-effective, IoT-sensor-based

system for continuous health monitoring. The system tracks vital signs like ECG, EMG, temperature, and pulse, along with environmental indicators. By seamlessly transmitting data to remote physicians, it enables real-time awareness of patients' physical conditions, enhancing healthcare services. techniques for authentication that are used to confirm the identification of users and devices that are transmitting data. To guarantee that only authorized parties can access sensitive medical information, this could include digital certificates issued by reliable agencies,

biometric verification, and multi-factor authentication (MFA).Regulations governing the handling of medical data in contexts of personalized healthcare should receive special consideration. This entails abiding by laws such as GDPR, HIPAA, and other local ordinances, which require the installation of strong security measures to safeguard patient confidentiality and data security.the significance of these security measures in promoting confidence and trust among stakeholders in personalized healthcare systems, including patients and healthcare practitioners. Organizations may guarantee the secure and smooth transfer of medical data by giving data security and regulatory compliance first priority, thereby improvingThe project envisions a future where healthcare is proactive, personalized, and seamlessly integrated with technology, providing richer and more dynamic patient records during check-ups.

3. REVIEW OF LITERATURE

A. Balasundaram, Sideward Rout Raya [1] Internet of Things (IoT)-Based Smart Healthcare System for Efficient Diagnostics of Health Parameters of Patients in Emergency Care Information about the current existing research and development of wireless biosensors system for effective health care monitoring. This system consists of wireless sensors using Zig-Bee wireless technology, and ultra-low power technology. This System also supports wireless communication for Wireless Body Area Network. Zhihua Xia et al. [2] An AES-based secure image retrival scheme using random mapping and bow in cloud computing The method involves encrypting images using Advanced Encryption Standard and block permutation, followed by generating random templates on the cloud server to extract local features. These features are then clustered using the k-means algorithm to create visual words, forming a histogram of encrypted visual words for each image. Similarity between images is determined by measuring the distance between their feature vectors. Experimental results demonstrate the effectiveness of the proposed scheme in maintaining privacy while retrieving images from the cloud.

Sudip Misra, Saswati Pal [3] i-AVR an IoT-based system designed to offer critical-aware recommendations for point-of- care during ambulance transit. It addresses delays caused by traffic congestion and distant hospitals by providing guidance for time-critical scenarios. i-AVR consists of a portable healthcare unit and an Android navigation unit. The healthcare unit computes patient criticality en-route and recommends the nearest healthcare center, while the navigation unit suggests optimal routes and monitors vital signs. The system demonstrates effective network performance, with computation and communication times in seconds and milliseconds.

Mohammad A. R. Abdeen et al. [4] Smart health is a relatively new paradigm where information and communication technology is utilized to improve health care and medical services. In this article, we provide a literature-based overview of smart health systems, their components, architecture, technologies, benefits, applications, challenges, and opportunities. In addition, we discuss the potential benefits of big data, data analytics, artificial intelligence, and machine learning in smart health systems. Moreover, we discuss the challenges as well as the open research issues that need further investigation to facilitate the implementation of smart health systems.

Mohammad A. R. Abdeen et al.[5] Smart Health Systems Components Challenges and Opportunities. A relatively recent concept called "smart health" uses information and communication technology to enhance medical services and healthcare. We present a literature-based review of smart health systems in this article, covering their elements, architecture, technologies, advantages, uses, obstacles, and prospects. We also go over the possible advantages of artificial intelligence (AI), machine learning (ML), big data, and data analytics in smart health systems.

Md. Milon Islam et al. [6] Device Capabilities Architectures Protocol and Smart Applications in Healthcare Domain. The Internet is affecting people's lives in ways never seen before, having extended to almost every nation on earth. Due to its many uses, the Internet of Things (IoT) is becoming more and more well-known, piqueing the curiosity of academics and practitioners alike in the era of wireless communication. The Internet of Things (IoT) is a technological advancement that makes ordinary objects smarter, ordinary computation more

intelligent, and ordinary communication slightly more perceptive. To give academics working in this field a comprehensive understanding of IoT technology, the most frequent and popular IoT device capabilities, designs, and protocols are briefly illustrated in this article. The typical IoT device functionalities, such as the Raspberry Pi, Arduino, and ESP8266 hardware and the operating.

L. Jih-Sheng et al [7] Multilevel converters-a new breed of power converters. A novel class of power converter alternatives for high-power applications is multilevel voltage source converters. The staircase voltage wave is usually synthesized by the multilevel voltage source converters from many layers of DC capacitor voltages. The voltage imbalance between levels is one of the main drawbacks of multilevel converters. Voltage clamping or capacitor charge control are common methods used to balance the voltage between various levels. Multilevel converters can incorporate voltage balancing in a number of ways. This study discusses three recently developed multilevel voltage source converters (i.e., diode-clamp, flying- capacitors, and cascaded-inverters with distinct DC sources) without taking into account the traditional magnetic linked converters

Amit Kumar Jaiswal et al. [8] Deep Learning-Based Smart IoT Health System for Blindness Detection Using Retina Images. Based on Deep Learning Because smart healthcare is applicable in real time to everyone's life, it is gaining a lot of attention. This attention has increased as IoT has come together. Among persons in their working years, diabetic eye disease is the leading cause of blindness. Millions of people live in the major Asian countries, including China and India, and the number of diabetics among them is rapidly rising. The increasing number of individuals with diabetes presented a significant problem for medical professionals who are trained in screening and diagnosing patients. Our objective is to use deep learning techniques to automatically detect blind spots in an eye and determine the potential severity of the condition. In this work, we provide an enhanced method based on recently published

B. D. Deebak Fadi Al-Turjman [9] Smart Mutual Authentication Protocol for Cloud Based Medical Healthcare Systems Using Internet of MedicalThings. Technological development expands the computation process of smart devices that adopt the telecare medical information system (TMIS) to fulfill the demands of the healthcare organization. It provides better medical identification to claim the features namely trustworthy, efficient, and resourceful. Moreover, the telecare services automate the remote healthcare monitoring process to ease professional workloads. Importantly, it is conceived to be more timesaving, economical, and easy healthcare access. Cloud-Based Medical Healthcare (CBMH) system is a standard platform that gives its support to the patients for emergency treatment from the medical experts over Internet communication. Krishna Prasad Sitamarhi, [10] A Secured Healthcare Model for Sensor Data Sharing with Integrated Emotional Intelligence. The Internet of Things has the potential to revolutionize medical treatments, diagnosis, and prognostication. By integrating IoT with healthcare, patients, families, doctors, and medical insurance companies may stay connected for proactive service delivery. However, because IoT devices operate in un-infrastructure environments, concerns about data security and privacy are ongoing. Counterfeit IoT devices are a major risk to vital applications. Moreover, conventional healthcare systems are not patient-centric because they do not take the patient's feelings into account when administering care. Physicians can better comprehend and oversee medical processes with the help of EI. This study integrates sensor networks based on Internet of Things (IoT) devices with emotional intelligence (EI) to introduce a human-centered strategy in the healthcare arena. sensors and a camera

4. PROPOSED SYSTEM

Sensors like Electro Cardiograph (ECG), Electromyography. (EMG), and Temperature and Pulse sensors are connected to the body with the help of ESP8266 Node MCU Microcontroller. There is inbuilt Wi-Fi module in the microcontroller. In the proposed system transmitting of encrypted data to the local server is done for security purpose, here Advanced Encryption standard (AES) algorithm is used for security purpose. Secure devices that can collect, process, and send medical data across wireless networks are part of the suggested system. These gadgets could

include smartphones, wearable health trackers, medical sensors, and Internet of Things (IoT) devices with secure communication protocols and encryption built in. Sensitive medical data is protected during transmission since every device is set up in accordance with industry standards for data security and privacy.

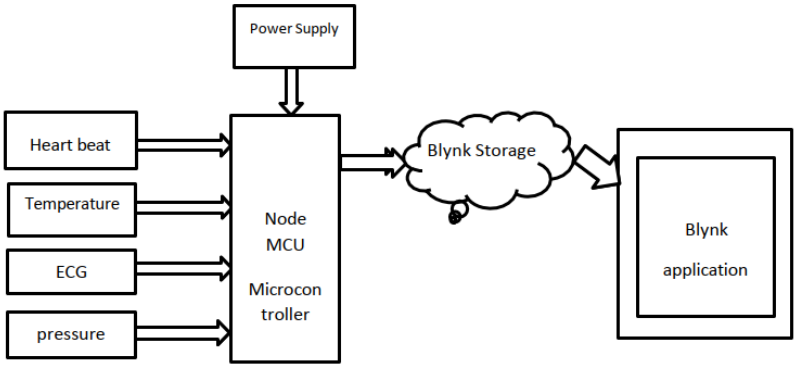


Fig 4.1 Proposed system block diagram

Medical Electronics is also going to advance with the application of the Internet of

Things.In this project, a simple patient health monitoring device is developed as an IoT application. The device could read pulse rate, measure the change in volume of blood through any organ, measure surrounding temperature and pressure, and continuously monitors the pulse rate and surrounding temperature and updates them to an IoT platform. The IoT project developed here is built on Node MCU.The device uses Node MCU that connects to the heartbeat, ECG, pressure and temperature sensor. It shows the heartbeat, ECG signal, pressure and temperature readings on LCD display and at the same time sends them to Blynk IoT platform in real-time via Wi-Fi and also the GSM Board will send the notification to the respective members. When any readings are uncommon, the system will send the notification to Line application. The android application can keep track of all measuring devices and community member records.

The hardware is implemented by using mat lab simulation. the proposed system emphasizes interoperability and scalability, allowing seamless integration with existing healthcare IT systems and accommodating future expansions and advancements in personalized healthcare technology. By leveraging state-of-the-art encryption techniques, robust authentication mechanisms, and secure communication protocols, the proposed system establishes a trustworthy and efficient framework for transmitting medical data wirelessly in personalized healthcare settings, ultimately enhancing patient outcomes and improving the quality of care.

5. IMPLEMENTATION

A crucial component of guaranteeing precise and instantaneous tracking of patients' health indicators is the integration of sensors into the safe wireless data transfer system for customized healthcare. The process of sensor integration entails the smooth integration of many physiological data-capturing sensors, including blood pressure, temperature, and heart rate, with the wireless communication infrastructure.

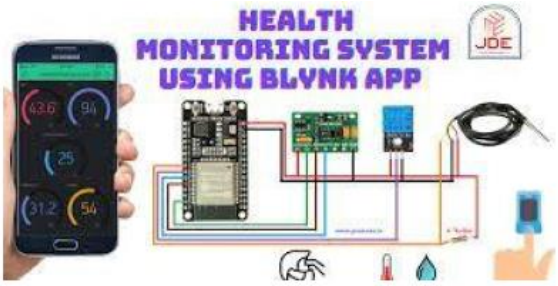


Fig. 5.1 CONNECTING SENSOR TO BLYNK IOT APPLICATION

It is crucial to maintain data security and integrity while it is being transmitted. To prevent unauthorized access or alteration, sensor data can be encrypted before transmission using encryption protocols like AES, SSL, or TLS.

Ensuring accurate and real-time monitoring of patients' health measurements is contingent upon the implementation of a secure wireless data transmission system for personalized healthcare. The process of sensor integration entails the smooth integration of multiple physiological data-capturing sensors with the wireless communication infrastructure. Examples of these sensors include blood pressure, temperature, glucose levels, and heart rate.

It is crucial to choose the right sensors based on the unique requirements of the healthcare system.

Different kinds of sensors may be needed for various medical situations. For instance, an electrocardiogram sensor may be necessary for a patient with heart problems, but a continuous glucose monitoring sensor may be advantageous for a patient with diabetes. It is therefore essential to comprehend medical requirements and select sensors that provide precise measurement of pertinent parameters. Furthermore, authentication measures can be put in place to confirm the legitimacy of the sensors and guarantee that the data can only be accessed by authorized devices. For quick and accurate real-time monitoring, dependable communication links between the sensors and the endpoints must be established.

6. RESULTS AND DISCUSSION

The result is the application of cutting-edge encryption techniques to safeguard medical data against illegal access or interception. Data is encrypted before transmission using methods like AES, SSL, and TLS, rendering it unreadable to anyone lacking the necessary decryption keys. This guarantees that the data will remain private and safe even in the event that it is intercepted. the use of strong authentication procedures to confirm the legitimacy of people and devices gaining access to medical data. Digital certificates, biometric verification, and multi-factor authentication (MFA) are used to guarantee that sensitive patient data is only accessible by authorized users and devices.

This lowers the possibility of data breaches and aids in preventing unwanted access. the creation of safe channels for communication using wireless technologies like WiFi



FIG 6. 1 Output of the project

Furthermore, the system optimizes data transmission protocols to minimize latency and ensure reliable delivery of data, even in scenarios with intermittent connectivity. This facilitates seamless integration with electronic health record systems or cloud- based healthcare platforms, enabling healthcare providers to access and analyze patient data in real- time.By combining sensor modules, ESP8266/ESP32 microcontrollers, and the Blynk IoT app, the project provides a scalable and cost- effective solution for personalized healthcare delivery while maintaining the highest standards of data security and privacy.

7. CONCLUSION

In conclusion, ensuring the secured wireless transmission of medical data in the realm of

personalized healthcare IoT is paramount for safeguarding patient privacy, maintaining data integrity, and mitigating potential risks. The multifaceted nature of this challenge demands a comprehensive approach that encompasses encryption, authentication, network segmentation, and ongoing vigilance. Implementing strong encryption protocols, robust authentication mechanisms, and network segmentation helps create a resilient defense against unauthorized access. Regular updates, both in terms of software and firmware, are essential to address emerging vulnerabilities.

Physical security measures, data integrity validation, and privacy protection mechanisms contribute to a holistic security posture. Furthermore, a proactive stance involves continuous monitoring, logging, and the development of emergency response plans to swiftly address security incidents. Adhering to data protection regulations and regularly conducting security audits and penetration testing ensures a proactive approach to identifying and rectifying vulnerabilities.

8. REFERENCES

1. A. Balasundaram, Sideward Rout Raya, Internet of Things Based Smart Healthcare System for Efficient Diagnostics of Health Parameters of Patients in Emergency Care,2023

2. Zhihua Xia, Jianwei Fei Feng xiao, An AES-based secure image retrival scheme using random mapping and bow in cloud computing ,2020.

3. Sudip Misra, Saswata, Palakkad, Mukherjee, Arijit Roy,Ananda Rup, i-AVR: IoT-Based Ambulatory Vitals Monitoring and Recommender System, 2023

4. Mohammad A. R. Abdeen, Dr. Abdeen, Dr. Ahmed, Tarek Rahil Shelta mi, Turki M. Alghamdi, Smart Health Systems Components Challenges and Opportunities,2022

5. Md. Milon Islam, Sheikh Nooruddin, Fakhri Karey, Ghulam Muhammad, Device Capabilities Architectures Protocol and Smart Applications in Healthcare Domain,2023

6. L. Jih-Sheng and P. Fang Zheng, "Multilevel converters-a new breed of power converters,2021

7. Amit Kumar Jaiswal, Prayag Tiwari, Sachin Kumar, Mabrouk Sal- Rahami, Mubarak Alresford, Ahmed Ghoneim, Deep Learning-Based Smart IoT Health System for Blindness Detection Using Retina Images,2021

8. B. D. Deebak Fadi Al-Turjman, Smart Mutual Authentication Protocol for Cloud Based Medical Healthcare Systems Using Internet of Medical Things,2021

9. Krishna Prasad Sitamarhi, Malarkodi Balakrishnan, A Secured Healthcare Model for Sensor Data Sharing with Integrated Emotional Intelligence,2022

10. Abdullah Ayub Khan, Sami Bourouis, M. Abruzzian, Myriam Hardjono, Zaffar Ahmed Shaikh, Asif Ali Laghari, Hela Elmina, Sami Dhabi, Data Security in Healthcare Industrial Internet of Things with Blockchain,2023