International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 SJIF 2023: 8.176 ISSN: 2582-3930

Secured IOT Healthcare

Sohan Dixit, Naresh Dewasi, Mahesh Pawle, Vaishanvi Mahajan, Shweta Bawiskar

Department of Computer Engineering
Genba Sopanrao Moze College of Engineering, Balewadi, Pune 45

Abstract - As wireless technology continues to grow in the healthcare industry, medical devices have become increasingly connected, enabling real-time monitoring and diagnosis for patients. However, this connectedness also poses security risks, putting sensitive data and patient safety at risk.

One solution to these vulnerabilities is the use of Body Sensor Networks (BSNs), which are designed to operate autonomously and connect various medical devices. BSNs utilize sensors and implants inside and/or outside the human body to provide opportunities for flexible operations and cost savings for both healthcare workers and patients.

The suggested system for BSNs includes an Android application and a Raspberry Pi unit with cloud connectivity and secure data access, providing real-time acquisition and analysis of various important parameters of the patient. By enabling seamless data collection, sharing, and storage, the system offers a high-quality patient experience while also supporting medical personnel in delivering effective care. Additionally, by eliminating manual data collection, the system helps to reduce human error and improve accuracy.

Overall, the implementation of intelligent health monitoring systems, such as BSNs, is a critical step towards ensuring patient safety and securing sensitive medical data. With the ability to collect, store, and analyze data in real-time, BSNs offer a unique service that can only be provided by a system that supports medical personnel from delivery to delivery.

Keywords - Body Sensor Network (BSN), Medical Devices, Wireless Technology, Security Vulnerabilities, Connectedness, Healthcare Sector, Real-time Monitoring, Data Analysis, Patient Safety, Cloud Connectivity, Android Application, Raspberry Pi, Intelligent Health Monitoring, Flexible Operations, Cost Savings, Manual Data Collection, Mass Monitoring

Introduction -

The use of medical devices has revolutionized healthcare, saved countless lives and improved patient outcomes. With the exponential growth of wireless technology, these devices have become increasingly connected to hospital networks, allowing for faster and more efficient patient care. However, this connectedness also opens numerous security vulnerabilities, putting patient safety and sensitive data at risk.

Body Sensor Networks (BSNs) have emerged as a solution to connect various medical devices, sensors, and implants inside and outside the human body, allowing for flexible operations and cost savings for both healthcare workers and patients. The design and implementation of intelligent health monitoring systems using BSNs can provide real-time acquisition and analysis of various important patient parameters, collect and share information seamlessly, and store information and records for future analysis.

Such a system can improve patient quality of care, providing medical personnel with real-time data to inform decision-making and eliminating manual data collection processes. By enabling mass collection and monitoring, patients can benefit from continuous health monitoring, resulting in better treatment outcomes and improved quality of life. However, the security of BSNs and the devices connected to them must be carefully considered to prevent cyberattacks and ensure patient safety.

LITERATURE REVIEW -

Sr. No.	Title	Features	Year	Strength	Limitations
1.	"A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications" by X. Li et al.	This survey paper provides an overview of the IoT architecture, enabling technologies, security and privacy issues, and applications.	2018	The paper provides a comprehensive survey of IoT-related topics, covering a wide range of areas. The authors have included a detailed discussion of the security and privacy challenges in IoT, which is a critical concern for IoT adoption.	As a survey paper, it may not delve into the technical details of individual topics. Also, the paper is a few years old, and some of the information may be outdated.
2.	"IoT Security: Review, Blockchain	The paper reviews the security challenges in	2019	The paper provides an in-depth analysis of the security challenges in IoT	The proposed solution is based on blockchain technology, which

	Solutions, and Open Challenges" by A. Dorri et al.	IoT and discusses how blockchain can be used to address these challenges. The authors also highlight the open research challenges in this area.		and proposes a blockchain-based solution. The authors have identified several open research challenges, which could guide future research in this area.	may not be suitable for all IoT applications due to its high computational overhead. Additionally, the paper does not provide a detailed evaluation of the proposed solution.
3.	"Towards a taxonomy of IoT devices" by S. Haddadi et al.	The paper proposes a taxonomy for IoT devices based on their functionality, connectivity, and power requirements.	2019	The paper provides a clear and concise taxonomy for IoT devices, which can be useful for researchers and practitioners working in this area. The authors have also included several examples to illustrate the taxonomy.	The proposed taxonomy may not capture all types of IoT devices, and there may be some overlap between the different categories. Additionally, the paper does not discuss the implications of the proposed taxonomy for IoT development or deployment.
4.	"An IoT-Based System for Flood Monitoring and Warning" by A. Garg et al.	The paper describes an IoT-based system for flood monitoring and warning, which uses wireless sensor networks and machine learning algorithms.	2017	The paper presents a real-world application of IoT technology, which could have significant social and economic impact. The authors have also included a detailed evaluation of the system's performance.	The proposed system may be expensive to deploy and maintain, which could limit its scalability. Additionally, the paper does not discuss the system's energy efficiency or its resilience to cyberattacks.
5.	"Smart Home Automation	The paper presents a smart home	2018	The paper demonstrates the potential of IoT	The proposed system may be vulnerable to cyberattacks, which

	System Using IoT" by S. Goyal et al.	automation system that uses IoT technology to control various home appliances.		technology in improving the quality of life for individuals by automating home tasks. The authors have also provided a detailed description of the system's architecture.	could compromise the security and privacy of the users. Additionally, the paper does not discuss the system's energy efficiency or the user experience of using the system.

RELATED WORK -

There have been several studies and developments related to patient monitoring and telemedicine systems. For example, developed a telemedicine monitoring system that utilizes physiological sensors such as temperature, pulse rate, and ECG. The system processes the acquired data using an ARM7 LPC 2138 processor and displays it on a Matlab user interface. An alarm SMS is sent to a doctor's mobile device if any of the critical parameters exceed normal levels. The system does not require specialized software on the PC.

Another example is the patient tracking and monitoring system. This system integrates vital sign sensors, location sensors, ad-hoc networks, electronic medical records, and web portals to enable communication between healthcare providers, doctors, and specialists from remote locations. This system is particularly useful for disaster management and can assist with triage in the event of a mass casualty disaster.

The healthcare industry's vision is to provide better healthcare to all individuals, regardless of their location, in a more patient-friendly and economic manner by using advanced technologies such as the Internet of Things (IoT). The use of IoT technology has great potential to transform the healthcare industry, particularly in patient monitoring. However, there are two major challenges that need to be addressed: the need for healthcare providers and caregivers to be physically present at the bedside of the patient and the fact that patients are often restricted to bed and wired to large machines.

To address these challenges, IoT-based patient monitoring devices can enable remote monitoring of patients, allowing healthcare providers to monitor patients' vital signs and health data from a remote location. Wearable patient monitoring devices that are smaller and more portable can provide real-time health data to healthcare providers, allowing them to monitor patients' health even when they are away from the bedside. By leveraging advanced technologies and developing more advanced, wearable patient monitoring devices, we can improve patient care efficiency and help to ensure that all patients receive the care they need, regardless of their location or physical condition.

PROPOSED SOLUTION -

1. Implementation of Secure Authentication: A secure authentication system should be implemented to ensure that only authorized individuals can access the patient's data. This can be done by using a two-factor authentication system that requires a password and a unique identifier, such as a fingerprint or an OTP (one-time password).
2. Data Encryption using AES Algorithm: All data that is transmitted between the patient monitoring device and the receiving device should be encrypted using the AES (Advanced Encryption Standard) algorithm. This will ensure that even if the data is intercepted by a third party, it will be unreadable.
3. Implementation of Secure Communication Protocol: The communication protocol between the monitoring device and the receiving device should be secure and encrypted. This can be achieved by using a secure communication protocol, such as TLS (Transport Layer Security) or SSL (Secure Sockets Layer).
4. Use of Secure Bluetooth: Bluetooth is a commonly used wireless communication technology in remote patient monitoring devices. To ensure the security of the data transmitted over Bluetooth, a secure Bluetooth protocol, such as Bluetooth Secure Simple Pairing (SSP) or Bluetooth Low Energy (BLE), should be used.
5. Use of Secure Storage: The patient's data should be stored securely to prevent unauthorized access. This can be done by using secure storage solutions, such as encrypted databases or cloud storage solutions with robust security features.

By implementing these measures, the remote patient monitoring system can ensure the security and confidentiality of the patient's data, as well as comply with privacy regulations and industry standards.

MATERIALS AND METHODS -

Platform - The Zigbee development platform based on Arduino Fio is an 8-bit platform that provides a development platform and means of code development. It is based on the ATmega328P AVR microcontroller and designed to understand all the basics of 8-bit microcontrollers. The Arduino Fio is specifically designed for wireless applications. Users can upload sketches (programs) using a USB cable or a modified USB to Xbee adapter such as the Arduino Fio Transmitter (Base). Programs can also be uploaded wirelessly with Xbee S1. The platform can be used for many projects, including wireless communication, robotics, and designing entertainment electronics

Temperature Sensor - The LM35 is a type of integrated circuit temperature sensor that can accurately measure temperature and convert it into a proportional voltage output. It is a precision device, meaning that it can provide accurate measurements with low errors, and it has a linear output that is directly proportional to

the temperature in Celsius. The LM35 sensor is commonly used in various electronic applications, including temperature measurement and control systems,

HVAC systems, automotive systems, and industrial process control. It can provide reliable and stable temperature measurements with a resolution of 0.1 degrees Celsius, making it ideal for applications where accuracy and precision are critical.

In the context of the sensor devices, you mentioned earlier, LM35 is likely being used to measure the temperature of a human body or some other object. The output of the sensor can then be processed by the Arduino Fio platform and transmitted wirelessly via Zigbee to a remote device for further analysis or monitoring.

Blood Pressure Sensor - For pulse rate measurement, an IR sensor pair is used which consists of an IR LED and photodiodes, also known as an optocoupler. The principle of the IR sensor is that the IR LED emits IR radiation, and the photodiodes capture this radiation. The amount of IR radiation received by the photodiode's changes depending on the blood flow and density of the skin tissue, which affects the photodiode resistance.

The resistance change causes a voltage drop, which can be detected using a voltage comparator (LM358). The output of the comparator changes depending on the voltage drop and provides a signal that can be processed to determine the pulse rate. By using this IR sensor pair, the pulse rate can be measured accurately and non-invasively, making it a useful tool in medical and health monitoring applications.

WORKING PRINCIPLES -

1. Connect the sensors to the Arduino Fio transmitter board as well as to the patient.
2. Acquire values from the sensors and store them in the form of an array.
3. Connect the Arduino Fio receiver to the system using USB.
4. Send the acquired parameters wirelessly to the receiver.
5. Restore the sensor values by typecasting from ASCII to normal.
6. Compare the values with threshold values to indicate any abnormal conditions.
7. Display the vital parameters on the front panel.
8. Receive values and encrypt the data using advanced algorithms.

CONCLUSION -

Based on the above process, it can be concluded that wireless transmission of medical sensor data can be achieved using Arduino Fio board and sensors. This method provides a cost-effective and easy-to-use solution for real-time monitoring of patients' vital signs. The use of threshold values and encryption algorithms can enhance the security and accuracy of the system. Overall, this wireless medical sensor network can provide a reliable and efficient solution for remote patient monitoring and can have significant applications in telemedicine and home healthcare.

REFERENCES -

[1] "Information, information all over", The Economist, 25 February 2010, accessible at http://www.economist.com/hub/15557443 (Downladed on April 30, 2012).

[2] E. Bertino, "Enormous Data - Opportunities and Challenges", Panel Position Paper, Proceedings of the 37th Annual IEEE Computer Software and Applications Conference, COMPSAC 2013, Kyoto, Japan, July 22-26, 2013.

[3] J. Manyika, M. Chui, J. Bughin, R. Dobbs, P. Bisson, and A. Marrs. Problematic innovations: Advances that will change life, business, and the worldwide economy. http://www.mckinsey.com/experiences/business innovation/disruptive_technologies, May 2013.

[4] E. Bertino, S. Nepal, R. Ranjan, "Building Sensor-Based Big Data Cyberinfrastructures", IEEE Cloud Computing 2(5): 64-69 (2015).

[5]. Atzori, M. (2017). Blockchain Governance and the Role of Trust Service Providers: The TrustedChainÂ® Network. Available online at: https://trustedchain.it/wp-content/uploads/2017/11/ ATZORI_-TrustedChainWhite-Paper.pdf.

[6]. Baars, D. (2016). Towards Self-sovereign Identity Using Blockchain Technology (master's thesis). University of Twente, Enschede, Netherlands.

[7]. Bandyopadhyay, P. (2018). The origin of blockchainfrom cypherpunks to Satoshi to IBM medium. Available onlineat: https://medium.com/datadriveninvestor/cypherpun ks-to- satoshi-to-ibm-819ebcfdd674.

[8]. Higgins, S. (2014). Factom outlines a record-keeping network that utilises bitcoin's blockchain. Coindesk. Available online at: https://www.coindesk.com/factom-white-paper-outl ines- record-keeping-layer-bitcoin.

[9]. Cheng, S., Duab, M., Domeyer, A., Lnudqvis, M.: Using blockchain to improve data management in the public sector. https://www.mckinsey.com/business-functions/digit almckinsey/our-insights/using-blockchain-to-improv e-data- management-in-the-public-sector.

[10]. Open Trading Network: UK police – blockchain solutions on the horizon. https://medium.com/@otncoin/uk-police-blockchai n- solutions-on-the-horizon- 60e3e1932ef3.