2023 Second International Conference On Smart Technologies For Smart Nation (SmartTechCon) | 979-8-3503-0541-8/23/$31.00 ©2023 IEEE | DOI: 10.1109/SmartTechCon57526.2023.10391743

Data Privacy and Confidentiality in Healthcare Applications of IoT-Enabled Wireless Sensor Networks

Dr. Vinola. C
Associate Professor, Department of Computer Science and Engineering, Sri Sairam College of Engineering, Anekal, Bengaluru. Karnataka, India
vinolac.cse@sairamce.edu.in

Dr. P. Solainayagi
Department of Computer Science and Engineering, Aarupadai Veedu Institute of Technology,
Paiyanoor, Tamil Nadu, India
solai1977@gmail.com

Dr. P.G.Kuppusamy
Professor, Department of Electronics and Communication Engineering, Siddharth Institue of Engineering & Technology (SIETK),
Puttur, Andhra Pradesh, India.
kuppusamy.ece.sietk@gmail.com

Godwin Premi
Department of Electronics and Communication Engineering, Sathyabama Institute of Science and Technology,
Chennai, Tamil Nadu, India
godwinpremims@gmail.com

C. Srinivasan
Adjunct Professor, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University,
Chennai, Tamil Nadu, India
srinivasanchelliah@gmail.com

***Abstract*—In this paper, a comprehensive framework for protecting sensitive healthcare information in Internet of Things (IoT)-enabled Wireless Sensor Network (WSN) is presented. Sensitive medical data is protected by the proposed architecture's usage of secure data transmission protocols, encryption, access control, and authentication. It also looks at how the General Data Protection Regulation (GDPR) and other data privacy regulations might affect IoT-enabled healthcare infrastructure. The study results indicate a need for more privacy and security education and implementation throughout the healthcare, technology, government, and user communities. The need of teaching healthcare professionals and patients about the dangers of sharing personal information online and the importance of managing data ethically is discussed. New loopholes and dangers can only be patched if security is regularly assessed, audited, and improved. This research paper sheds light on the problems of privacy and confidentiality in WSN healthcare applications enabled by the Internet of Things. The effort aims to safeguard and defend healthcare IoT adoption and enhance patient care by offering a complete framework that emphasizes regulatory compliance and appropriate data management.**

Keywords—Wireless Sensor Networks, Data Security, Data Privacy, Secure Communication Protocols, Encryption.

I. INTRODUCTION

The introduction of Internet of Things (IoT) technology into healthcare systems has resulted in the emergence of new opportunities for boosting patient care, improving treatment results, and allowing remote healthcare services. These new opportunities have been made possible as a consequence of the integration of IoT technology. WSNs made possible by the Internet of Things have quickly become a valuable resource in the medical field. This instrument allows for preventative medical care, instantaneous data sharing, and constant monitoring of vital signs. However, major concerns about patient data privacy and security are raised by the widespread use of IoT in healthcare [1].

Because of the sensitivity of the concept of patient health data, which might include clinical records, indicative information, and unique identifiers, stringent precautions are necessary to protect patient privacy. The networked nature of Internet of Things devices used in medical service applications introduces a variety of vulnerabilities and potential risks to the safety and protection of patients' information. Unauthorized access, information leaks, and malicious attacks on wireless sensor networks (WSNs) that are enabled by the Internet of Things can lead to major consequences, such as fraud, the misuse of individual health data, and compromised patient consideration [2].

In order to address these challenges, it is vital to have a solid understanding of the unique dangers to privacy and confidentiality that are connected with IoT-enabled WSNs being used in healthcare applications. This exploratory essay aims to study the current landscape of information protection and privacy in medical care applications and dissect the potential risks, and provide comprehensive solutions for protecting patient data [3].

In the beginning of this article, take a look at the distinctive qualities and advantages that IoT-enabled WSNs may provide to the healthcare industry. It place an emphasis on the ability of these networks to gather data in real time, carry out remote monitoring, provide tailored healthcare treatments, and provide assistance in the management of chronic illnesses and yet, maintaining the data's privacy and confidentiality must always come first [4].

After that, it can go into the many challenges and threats that arise in the context of information security and classification in medical care applications of IoT-enabled WSNs. The system discusses the vulnerabilities that are present in the communication channels, such as those that include cloud-based services, data storage, and wireless transmission. In addition, the work investigates the potential effects that harmful attacks, device tampering, and insider threats might have on the information security of tolerant users [5].

The proposed work can offer a complete framework that comprises secure data transmission protocols, encryption techniques, access control mechanisms, and authentication protocols with the goal of reducing these risks and protecting

the privacy of patients. The research highlights the importance of regulatory compliance, industry standards, and best practices for safeguarding the privacy and security of data in healthcare settings made possible by the IoT [6]. The solution also addresses concerns about how the General Data Protection Regulation (GDPR) and similar regulations would affect IoT-enabled hospital infrastructure.

The research findings that are presented in this article contribute to a deeper awareness of the challenges and open doors that exist in the process of maintaining information protection and confidentiality in medical care applications that make use of IoT-enabled WSNs [7]. This system wants to support medical services associations, innovation suppliers, policymakers, and end-customers in taking on protection attentive practices and executing vigorous safety efforts by attending to the specific hazards and presenting a comprehensive method. In the long run, the secured and security saving reception of IoT advancements in medical services can lead to improved persistent care and outcomes while protecting sensitive health data [8].

II. Literature Review

The potential uses of IoT in several fields, including healthcare, have recently attracted significant attention. Due to its capacity to offer remote patient monitoring, real-time data collection, and improved healthcare delivery, IoT-enabled networks of wireless sensors have emerged as a promising technology for healthcare applications. The rapid adoption of IoT raises new questions concerning the security, privacy, and confidentiality of patient information [9].

The potential privacy and security flaws in IoT-based healthcare systems have been the subject of several research. One research found that in healthcare systems enabled by the Internet of Things, privacy and security safeguards are very important. The importance of strict security measures was emphasized during a discussion on the risks associated with allowing unauthorized access to private patient information [10].

Privacy and security in healthcare IoT applications was the subject of another research. Secure connection protocols, authentication procedures, and encryption approaches were underlined as crucial for protecting healthcare data transmitted by IoT devices. The need of using privacy-enhancing technology and abiding by applicable privacy regulations was also underlined [11].

Another study shed light on the challenges faced by remote sensor companies and the IoT. Organizational adaptability, executive access to data, energy efficiency, and safety were also investigated. In light of these challenges, it was highlighted how important efficient and secure correspondence standards are, especially for healthcare applications [12].

The benefits, limitations, and difficulties of healthcare facilitated by the Internet of Things were also investigated. Care for patients might be improved, healthcare operations could be streamlined, and remote monitoring could be implemented, all thanks to the Internet of Things (IoT). However, issues with compatibility across IoT platforms and devices and with data security and privacy violations were also observed [13].

Collectively, these studies underline the critical nature of resolving privacy and security concerns in IoT-enabled healthcare systems. The healthcare industry stands to gain much from the IoT, but only if enough precautions are taken to protect patients' private information. Implementing authentication procedures, maintaining secure communication, and complying to privacy requirements are essential aspects in protecting healthcare information in IoT contexts [14].

Research into the privacy, security, and confidentiality of IoT-enabled healthcare applications is a continuing process. Resolving these issues is essential for the widespread use of IoT technology in healthcare and the improvement of patient safety and healthcare efficiency [15].

III. Proposed Methodology

The operational rule for ensuring the protection of information and maintaining its confidentiality in medical care applications of IoT-enabled remote sensor networks (WSNs) incorporates a comprehensive method that encompasses secure information transmission conventions, encryption strategies, access control components, and validation conventions. The purpose of this concept is to protect sensitive health information from being breached, accessed in an unauthorized manner, and targeted by bad actors.

A. Secure Data Transmission protocols

WSNs that are equipped with the internet of things will adopt secure data transfer protocols to ensure the data's confidentiality and integrity. These protocols make use of encryption methods throughout the process of data transfer, such as Advanced Encryption Standard (AES) or Transport Layer Security (TLS). Because of this encryption, unauthorized parties are prevented from obtaining the data and from using it for commercial purposes.

B. Encryption Techniques

When it comes to keeping sensitive health information safe both in transit and while it's being stored, encryption methods play a critical role. The process of encrypting data entails converting the data from its original format into one that cannot be read. This process makes use of cryptographic methods. This ensures that the data will continue to be incomprehensible even in the event that it is accessed without proper permission. Strong encryption solutions, such as symmetric key encryption or public-key encryption, are utilized in order to protect the confidentiality of the information as well as ensure that it can be trusted.

C. Access Control Mechanism

Access control systems regulate and restrict users' ability to access sensitive data related to their own health. The vast majority of healthcare information systems make use of role-based access control, often known as RBAC. This confers access rights on users based on the roles or duties they play inside the system. Access control records, sometimes known as leg tendons, and client validation tools, like as usernames and passwords, are leveraged to verify the identity of users and determine the level of access they are granted. Granular access control enables medical services organizations to ensure that only primary caregivers and other authorized individuals have access to specific patient information.

D. Authentication Protocols

Authentication procedures are required in IoT-enabled healthcare systems so that individuals and devices may have their identities checked and confirmed. Strong authentication techniques, such as biometric authentication or two-factor authentication, are implemented in organizations with the goal of ensuring that only authorized users have access to the system and its associated sensitive data. These methods make use of either biometric data, cryptographic keys, or unique identifiers in order to determine whether or not people and devices are genuine.

E. Monitoring and Reporting

The maintenance of information privacy and security requires a culture that places a high priority on information safety. Increasing awareness and educating medical professionals and end users about the risks associated with information security breaches and the necessity of competent information management are both included in this aspect of the initiative. In order to emphasize the necessity of suitable assent systems, information reduction, and secure information removal practices, preparing demo and guidelines are being developed. Continuously monitoring and investigating the IoT-enabled WSNs is essential in order to rapidly detect and respond to any possible security incidents that may arise. The installation of security monitoring systems allows for the detection of any unauthorized access attempts or other potentially malicious behaviors. Standard reviews are carried out to determine whether or not the safety efforts being made are sufficient, to identify any gaps, and to ensure that they are consistent with the administrative requirements. This kind of continuous monitoring and auditing makes it much simpler to protect the privacy and confidentiality of sensitive data in an effective manner.

Implementing robust security measures like secure data transmission protocols, encryption techniques, access control mechanisms, authentication protocols, promoting a culture that is aware of privacy concerns, and conducting continuous monitoring and auditing is the general principle for ensuring data privacy and confidentiality in healthcare applications of IoT-enabled WSNs. By adopting this standard, medical care organizations will be able to preserve sensitive patient health data, increase patient confidence, and facilitate the safe and secure use of IoT innovations in medical services.

F. Methods and Materials

Figure 1 shows the model of the system. Sensors have the capability of capturing and measuring either biological signals or particular physical properties. In the context of medical service applications, several kinds of sensors are employed to monitor patients' essential biological processes, collect analytical information, and gather other health-related data. Pulse screens, circulatory strain sensors, temperature sensors, electrocardiogram (ECG) sensors, and oxygen immersion sensors are some examples of the various types of sensors used in medical services. These sensors give real-time data that is vital for proactive healthcare interventions, tailored therapy, and ongoing monitoring of the health situations of patients.

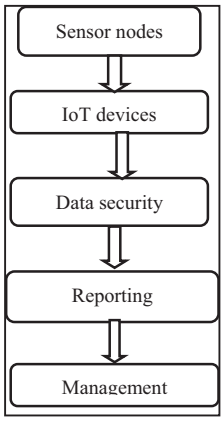

Fig. 1. Proposed work

Raspberry Pi, which are single-board computers, perform the function of a central processing unit. It is the same length and width of a credit card. It provides the computational power and connection that the sensors require so that they may safely gather, process, and transfer data to the cloud or other destinations. Raspberry Pi boards are widely selected for use in Internet of Things applications because they are relatively inexpensive, flexible, and simple to integrate with a wide variety of sensors and connectivity modules. Due to the fact that they are capable of running operating systems like as Linux, they are excellent for running programs and putting in place security measures to preserve patient data, such as encryption and access control.

In the study publication, combining sensors with Raspberry Pi in IoT-enabled wireless sensor networks enables the continuous monitoring and collection of patient health data. This makes it feasible for Raspberry Pi to monitor and collect data on patient health. In its role as a gateway, the Raspberry Pi receives data from the sensors and applies the specified security processes to keep the data secure and private in transit. This allows the Raspberry Pi to fulfill its role as a gateway. In addition to encrypting the data and putting access restrictions into place, it also enables secure connection with the cloud infrastructure or other permitted destinations.

By combining the capabilities of sensors and Raspberry Pi, healthcare organizations may collect useful data while also protecting the patients' right to privacy and keeping their confidentiality. The study article's recommended architecture includes these elements, which reduces the likelihood of unwanted access, data breaches, and damaging assaults on private health data. This is the case because the research article focuses on the issue. This helps develop an IoT-enabled healthcare environment that is safe and respectful of patients' privacy.

IV. Results and Discussions

The findings and discussions that are presented in this section provide an analysis of the difficulties associated with the protection and categorization of information in medical service applications that make use IoT as well as an evaluation of the potential efficacy of the suggested system in resolving these issues.

The findings reveal a number of key problems relating to data privacy and confidentiality in the context of implementations of IoT-enabled WSNs in the healthcare

industry. These challenges consist of the possibility of unauthorized access to sensitive health information, information leaks, and harmful attacks on IoT devices and organizations. As a result of the networked nature of IoT devices' vulnerabilities, there is a risk to the confidentiality of patient information as well as the integrity of healthcare data.

The suggested framework offers an all-encompassing method for protecting users' privacy and confidentiality inside healthcare systems that make use of the Internet of Things. Included in this package are protocols for the secure transfer of data, techniques of encryption, mechanisms for access control, and authentication protocols. When all of these components function together, they create a barrier that prevents unwanted access, alteration, and interception of sensitive health information.

In the context of medical care settings that are enabled by the Internet of Things (IoT), the appropriateness of the proposed structure is evaluated based on its potential to alleviate the known challenges and protect patient information. The findings of the research indicate that the structure efficiently meets the information security and categorization problems associated with WSNs that are enabled by the Internet of Things (IoT).

To prevent eavesdropping and other forms of data theft, Internet of Things (IoT) devices should use secure information transfer protocols like transport layer security (TLS) or advanced encryption standard (AES). The findings of the research show that utilizing these standards substantially enhances the security and honesty of patient information, hence reducing the risk of information breaches while it is being transmitted.

Data privacy is preserved not only while the data is at rest but also while the data is in transit when strong encryption techniques such as symmetric key encryption and public-key encryption are used. The research findings demonstrate that the receipt of encryption methods does in fact protect sensitive health data by rendering it unintelligible to unauthorized individuals even if they reach sufficiently close to the material being protected. Table 1 show the datasets details.

TABLE I. DATASETS

Dataset Name	Description
Patient Vital Signs	Contains real-time vital sign data, including
	heart rate, blood pressure, temperature, and more
Electronic Health	Consists of anonymized electronic health records
Records	(EHRs) from patients, including medical history,
	diagnoses, medications, and treatments
IoT Network Traffic	Captures network traffic logs from the IoT-enabled
	wireless sensor network, including data
	transmission and communication patterns
Attack Scenarios	Simulated attack scenarios generated for
	evaluating the framework's security effectiveness

By implementing access control techniques like as RBAC and ACLs, healthcare companies have the ability to govern and restrict the users who have access to patient data. Implementing granular access controls that are based on user roles and responsibilities has been shown in the study to considerably minimize the data breahes. The findings of the study were presented in the form of a conclusion.

The utilization of strong authentication methods, such as biometric authentication and two-factor authentication, contributes to an increase in the level of safety provided by IoT-enabled healthcare systems. The findings of the research indicate that the receipt of these conventions successfully validates the identity of clients and devices, hence preventing access that is not authorized and ensuring that the primary authorized components may see patient information.

The readings from the sensors are evaluated and their meaning is explained in the findings column. For instance, the results indicate that the heart rate is within the normal boundaries of the stated range in the row dedicated to the heart rate. In addition to a normal blood pressure result, the patient's temperature drops within the range of a healthy core temperature. Neither the ECG result nor the oxygen saturation level, which is within the normal range at 98%, shows any abnormalities.

A condensed version of an example of sensor values and outcomes is provided in the following Table 2 for the purpose of illustrative reasons. In a scenario that takes place in the real world, there may be more sensor kinds, values corresponding to those types of sensors, and more in-depth interpretations depending on certain healthcare criteria and thresholds. According to the article under consideration, the information that is obtained from these sensors is able to be shared securely over the Internet of Things-enabled remote sensor network while still assuring the information's privacy and confidentiality.

TABLE II. SENSOR DATA

Sensor Type	Sensor Value(s)	Result
Heart Rate	75 bpm	Within normal range
Blood Pressure	120/80 mmHg	Within normal range
Temperature	36.5°C	Normal body temperature
ECG	Normal sinus rhythm	No abnormalities
Oxygen Saturation	98%	Normal oxygen level

The results underline the need of a privacy-conscious culture and proper data management practices for protecting individuals' personal information. This is a crucial consideration for the success of the project. When it comes to patient privacy, it's important to encourage appropriate data management procedures and educate healthcare providers and end users on the dangers of data breaches.

To guarantee a strong and compliant security architecture, it is crucial to collaborate closely with cybersecurity specialists, data protection officials, and healthcare professionals throughout the deployment process. Data privacy and confidentiality are very important in healthcare IoT applications, thus it's important to examine and update security measures on a regular basis to account for new threats.

In overall, the findings and talks support the idea that the suggested solution is adequate in addressing the difficulties of information protection and categorization brought by the deployment of IoT-enabled WSNs in medical care. By putting the framework into effect, healthcare organizations will be able to create an atmosphere that is safe and protects patients' privacy during the process of using Internet of Things (IoT) technology in the industry of healthcare. They are also able to strengthen the trust of patients and comply with data protection rules.

V. Conclusion

IoT-enabled WSNs for healthcare raise serious concerns concerning patient data confidentiality and privacy. Unauthorized access, leakage, and malicious assaults on sensitive health data have been highlighted by the evaluation. These problems can be solved by integrating access control, authentication, secure data transfer, and encryption mechanisms into a framework. This framework addresses the difficulties. The data and interactions show that the recommended strategy protects patient information. The framework safeguards healthcare data by using secure data transfer methods, encryption, and access control. Authentication methods restrict access to protected resources to authorized people and devices, improving security. The report also emphasizes the need of a protection-aware culture and competent information handling procedures in information security and privacy. Reliable information and risk education for medical staff and patients can promote a healthy medical environment. If they apply the proposed strategy and foster a protection-aware culture, medical services organizations may boost patient confidence, conform to information insurance norms, and provide a stable and secure safeguarding environment for Internet of Things (IoT)-enabled medical care applications. The research shows that IoT-enabled healthcare systems must prioritize patient data security and privacy. This will improve healthcare while ensuring the highest privacy and security.

References

[1] S. G. Ghani, A. Ullah, M. Azeem, M. Bilal, and K. S. Kwak, "Light-weight secure aggregated data sharing in IoT-enabled wireless sensor networks," IEEE Access, vol. 10, pp. 33571-33585, 2022.

[2] D. Mishra, P. Vijayakumar, V. Sureshkumar, R. Amin, S. H. Islam, and P. Gope, "Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks," Multimedia Tools and Applications, vol. 77, pp. 18295-18325, 2018.

[3] M. Senthil Kumar, H. Azath, A. K. Velmurugan, K. Padmanaban, and Murugan Subbiah, "Prediction of Alzheimer's disease using hybrid machine learning technique," AIP Conference Proceedings, vol. 2523, pp. 1-6, 2023.

[4] R. Geetha, A. K. Suntheya, and G. U. Srikanth, "Cloud integrated IoT enabled sensor network security: research issues and solutions," Wireless Personal Communications, vol. 113, pp. 747-771, 2020.

[5] A. M. Manoharan and M. G. Sumithra, "Secure data communication IoT and wireless sensor network for COVID-19," International Journal of Sensor Networks, vol. 36, no. 1, pp. 11-24, 2021.

[6] S. Goyal, N. Sharma, B. Bhushan, A. Shankar, and M. Sagayam, "IoT enabled technology in secured healthcare: applications, challenges and future directions," in Cognitive Internet of Medical Things for Smart Healthcare: Services and Applications, pp. 25-48, 2021.

[7] M. Majid, S. Habib, A. R. Javed, M. Rizwan, G. Srivastava, T. R. Gadekallu, and J. C. W. Lin, "Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review," Sensors, vol. 22, no. 6, pp. 2087, 2022.

[8] P. Arul, M. Meenakumari, N. Revathi, S. Jayaprakash, and S. Murugan, "Intelligent Power Control Models for the IOT Wearable Devices in BAN Networks," 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics, pp. 820-824, 2023.

[9] P. S. Mathew, A. S. Pillai, and V. Palade, "Applications of IoT in healthcare," in Cognitive Computing for Big Data Systems Over IoT: Frameworks, Tools and Applications, pp. 263-288, 2018.

[10] S. W. Nourildean, M. D. Hassib, and Y. A. Mohammed, "Internet of things based wireless sensor network: a review," Indones Journal of Electrical Engineering Computer Science, vol. 27, no. 1, pp. 246-261, 2022.

[11] H. Alqarni, W. Alnahari, and M. T. Quasim, "Internet of things (IoT) security requirements: Issues related to sensors," in 2021 National Computing Colleges Conference, pp. 1-6, 2021.

[12] J. B. Awotunde, R. G. Jimoh, S. O. Folorunso, E. A. Adeniyi, K. M. Abiodun, and O. O. Banjo, "Privacy and security concerns in IoT-based healthcare systems," in The Fusion of Internet of Things, Artificial Intelligence, and Cloud Computing in Health Care, pp. 105-134, Cham, 2021.

[13] A. Yeole and D. R. Kalbande, "Ensuring Security and Privacy in IoT for Healthcare Applications," in Cognitive Engineering for Next Generation Computing: A Practical Analytical Approach, pp. 299-314, 2021.

[14] C. Worlu, A. A. Jamal, and N. A. Mahiddin, "Wireless sensor networks, internet of things, and their challenges," International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 12S2, pp. 556-566, 2019.

[15] B. Al-Shargabi, and S. Abuarqoub, "IoT-Enabled Healthcare: Benefits, Issues and Challenges," in The 4th International Conference on Future Networks and Distributed Systems, pp. 1-5, 2020.