Enhancing IoT Healthcare Security Through No Zero Trust Architecture (NZTA): A Focus on Real-Time Pacemaker Monitoring

M.Ishwarya Niranjana[1*], Logitha Luckshmi.V.J[2], Manoj Jegan.D[3], Niranjan.D[4], Raksana Sri.S[5], Parthipan.V[6]

[1,2,3,4,5,6]Department of Electronics and Communication Engineering, Sri Eshwar College of Engineering Coimbatore, Tamil Nadu,India

[1*]ishwaryaniranjana.m@sece.ac.in
[2]logithaluckshmi.vj2022ece@sece.ac.in
[3]manojjegan.d2022ece@sece.ac.in.
[4]niranjan.d2022ece@sece.ac.in
[5]raksanasri.s2022ece@sece.ac.in
[6]parthipan.v@sece.ac.in

Abstract. Patient monitoring has been greatly enhanced by the use of Internet of Things (IoT) technologies in healthcare, particularly concerning pacemakers and other implantable medical devices (IMDs). This project presents an innovative IoT-based framework for monitoring patients with pacemakers using a heartbeat sensor connected to a NodeMCU microcontroller. Unlike traditional systems, which often lack robust security measures, our approach incorporates the No Zero Trust Architecture (NZTA) to enhance cybersecurity, ensuring that every data exchange is authenticated and monitored, thereby reducing vulnerabilities to cyber threats. Healthcare professionals can remotely monitor patients and provide immediate alarms for anomalous cardiac activity and possible magnetic interference by sending real-time data to cloud platforms like ThingSpeak or Adafruit IO. This novel implementation addresses the increasing cybersecurity risks associated with IMDs, as highlighted in existing literature that outlines the potential for malicious attacks on these devices. By leveraging NZTA principles, our system fosters a secure communication environment, significantly enhancing patient safety and data integrity compared to existing IoT solutions in the healthcare sector. This study highlights how crucial it is to incorporate cutting-edge cybersecurity safeguards into IoT healthcare applications, opening the door for more robust and reliable methods for medical monitoring.

Keywords: IoT, Pacemakers, Implantable Medical Devices, Cybersecurity, No Zero Trust Architecture

© The Author(s) 2025
S. K. Swarnkar et al. (eds.), *Proceedings of International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICSHIT 2024)*, Advances in Intelligent Systems Research 190,
https://doi.org/10.2991/978-94-6463-704-5_12

1. INTRODUCTION

Given that heart conditions continue to be a major global source of morbidity and death, the role of implantable medical devices, particularly pacemakers, has become increasingly significant. Pacemakers are sophisticated devices designed to regulate heart rhythms and enhance the sufferer's quality of life from arrhythmias. However, the Conventional techniques for keeping an eye on these devices frequently fail in terms of efficiency and timeliness. Regular check-ups and hospital visits are required to ensure proper device functionality, but these methods can lead to delayed responses to critical alterations in a patient's state[1].

Internet of Things (IoT) technology is advancing quickly, opening the door for creative healthcare solutions that can address these challenges. IoT-enabled devices allow for continuous and real-time monitoring of patient health data, thereby facilitating timely interventions when necessary [2]. The creation of an Internet of Things-based pacemaker monitoring system is the main goal of this project that integrates a heartbeat sensor with a NodeMCU microcontroller, providing a seamless connection to cloud platforms such as ThingSpeak or Adafruit IO for real-time data transmission and monitoring.

Incorporating a cloud-based framework allows Remote access to patient data by healthcare providers, enhancing the efficiency of care delivery and patient management [3]. Furthermore, the system aims to incorporate a robust cybersecurity framework based on the No Zero Trust Architecture (NZTA) to safeguard against potential cyber threats. Given the increasing connectivity of medical devices, cybersecurity is a critical aspect that need to be given top priority in order to safeguard private patient information and device functionality[7].

The proposed IoT-based Pacemaker Monitoring System not only enhances patient care but also emphasizes the need for a secure, reliable framework that mitigates the risks associated with cyber vulnerabilities. By leveraging IoT technology, this system promises to revolutionize how pacemaker patients are monitored, leading to improved outcomes and safety in an increasingly digital healthcare landscape [17].

2. LITERATURE SURVEY

IoT-Based Patient Health Monitoring System [1]

Mohamed et al. (2018) demonstrate the integration of multiple sensors and devices to gather health metrics in a thorough design and development of an Internet of

Things-based patient health monitoring system. The paper emphasizes the significance of real-time monitoring for improving patient outcomes, particularly in chronic disease management. By leveraging cloud technologies, the proposed system offers remote access to health data, facilitating timely interventions. The knowledge gathered from this research can help create comparable systems that concentrate on particular health metrics, such oxygen saturation and heart rate.

Healthcare Security in IoT [2]

Owais and Kalra (2019) delve into the challenges and solutions associated with healthcare security in IoT environments. Their work identifies vulnerabilities in IoT devices and proposes a robust security framework to safeguard patient data. This paper highlights the need for effective methods for authentication and encryption to stop illegal access and data breaches, which are critical for IoT-based health monitoring systems. Understanding these security challenges will be essential for developing a reliable pacemaker monitoring system that ensures patient data confidentiality.

Cloud-Based IoT Framework for Remote Patient Monitoring [3]

Alzahrani et al. (2020) present an IoT framework for remote patient monitoring that is cloud-based, showcasing its effectiveness in managing patient health data. The framework enables real-time data gathering and processing, which improves healthcare practitioners' ability to make decisions. The authors provide insights into the use of various communication protocols and cloud services for data transmission. This paper serves as a valuable reference for integrating cloud technologies in healthcare applications, particularly in the context of monitoring vital signs like heart rate and SpO2.

Cybersecurity for Medical Devices [4]

Rao and Gupta (2018) address cybersecurity for medical devices, focusing on the importance of protecting sensitive patient information. They discuss various threats and vulnerabilities associated with medical devices in healthcare settings and propose strategies to mitigate these risks. The findings underscore the necessity for incorporating strong security measures in IoT health monitoring systems. This research provides a foundational understanding of the security aspects that must be considered when developing IoT applications for monitoring critical health metrics.

Design and Implementation of Heart Rate Monitoring System [5]

Mohamad et al. (2020) examine the development and deployment of an IoT-based heart rate monitoring system. The study details the architecture and components required for

real-time heart rate measurement, emphasizing the importance of data accuracy and reliability. The authors also discuss the integration of mobile applications for user-friendly access to health data. This paper contributes valuable insights into the practical aspects of implementing heart rate monitoring systems, which can be adapted for a broader range of vital sign measurements.

Secure Data Sharing in IoT Healthcare Systems [6]

Shafique et al. (2021) examine how blockchain technology can be used to share data securely in Internet of Things-based healthcare systems. They propose a decentralized approach to enhance data integrity and confidentiality while facilitating seamless information exchange among healthcare providers. The emphasis on data security and patient privacy aligns with the increasing need for secure healthcare solutions. This work presents a potential avenue for incorporating advanced security measures in IoT health monitoring systems, particularly in the context of sensitive health data.

Patient-Centric IoT Health Monitoring [7]

Ahmad and Ahmad (2018) present an IoT-based health monitoring system that incorporates patient feedback mechanisms. Their study highlights the importance of user engagement in the healthcare process, enabling patients to provide instantaneous health status feedback. Better judgements are made as a result of the suggested system's improved patient-provider communication. This approach can be particularly beneficial for monitoring chronic conditions and encourages the integration of patient-centric features in IoT health monitoring applications.

Proactive Healthcare Management [8]

Alam et al. (2020) discuss the development of an IoT-based smart healthcare system that utilizes various sensors to monitor patient health parameters. The authors emphasize the importance of data collection and analysis for proactive healthcare management. According to their research, IoT systems have the potential to enhance patient outcomes by offering ongoing monitoring and early health issue detection. This work informs the design of IoT applications focused on real-time health monitoring, particularly in critical health scenarios.

IoT-Based Heart Rate Monitoring [10]

Nazari and Dunne (2021) examine heart rate monitoring using IoT technology, focusing on its applications in cardiac health management. Their research discusses various methodologies for accurate heart rate measurement and the consequences for medical

treatment. The study emphasises how crucial it is to incorporate real-time monitoring features in order to enhance cardiac health outcomes. This study serves as a relevant reference for developing IoT-based solutions that address specific health metrics, contributing to enhanced patient management strategies.

3. PROPOSED WORK

The IoT-based pacemaker monitoring system with security against cyberattacks is developed through several steps, focusing on real-time heart rate monitoring, secure data transmission, anomaly detection, and continuous improvement. These steps include,

Step 1: Requirements Analysis

Analyse the specific needs of the pacemaker monitoring system, with a focus on IoT integration and cybersecurity. The key requirements include real-time monitoring of patient heart rate, secure transmission of data, anomaly detection, and alerts for both medical and cybersecurity threats.

Step 2: Design the User Interface (UI)

Wireframes and design mockups for the user interface are created to visualize how healthcare providers and authorized users will interact with the system. The UI needs to be simple, responsive, and accessible across devices like desktops, tablets, and mobile phones. HTML and CSS are used to structure and design the interface, which displays real-time heart rate data collected from the IoT-based pacemaker.

Step 3: Creating the Front-End

The front-end of the system is built using HTML for the page structure and CSS for styling. JavaScript is integrated to enable real-time data visualization from the IoT pacemaker. The user interface focuses on presenting the heart rate data in an intuitive manner, showing visual indicators for normal and abnormal readings, and ensuring ease of access to healthcare providers for quick decision-making.

Step 4: IoT Device Setup and Configuration

The hardware setup starts by connecting the heart rate sensor to the NodeMCU microcontroller. The NodeMCU is programmed to read heart rate data in real-time and process it locally. The code involves collecting sensor data and preparing it for secure transmission. MQTT (Message Queuing Telemetry Transport) over SSL is configured for

secure data communication between the pacemaker system and the ThingSpeak cloud server.

Step 5: Database Design and Setup

Configure the ThingSpeak cloud platform as the storage and visualization tool for heart rate data. A dedicated ThingSpeak channel is created, where fields are defined to store heart rate data and corresponding timestamps. API keys are used to securely access and update the data in the ThingSpeak cloud, ensuring only authorized devices and users can interact with the platform.

Step 6: Implementing Business Logic

The core business logic is programmed into the NodeMCU, including secure transmission of heart rate data, anomaly detection, and the application of the No Zero Thrust Architecture (NZTA) for enhanced IoT security. This architecture ensures that all communication between the pacemaker, cloud, and users is verified and encrypted. The system uses AES encryption to secure heart rate data before transmission via MQTT over SSL. NZTA is employed to continuously monitor for cyberattacks and ensure no unauthorized access occurs, adding an extra layer of protection to the patient data. The logic also includes real-time alerts for abnormal heart rates or any detected cybersecurity threats.

Step 7: Examining and Quality Assurance

The pacemaker monitoring system is tested to ensure data is transmitted securely via MQTT over SSL, and that ThingSpeak correctly stores and visualizes the data. Security tests are conducted to ensure the system is resilient to common cyberattacks, such as data interception or tampering. The anomaly detection feature is also tested to verify it accurately triggers alerts when abnormal heart rates are detected.

Step 8: Documentation

Comprehensive documentation is prepared, covering the system architecture, setup, and usage guidelines. This includes: Instructions for configuring the NodeMCU and heart rate sensor, Steps to set up and secure the ThingSpeak channel, Code documentation explaining the encryption and MQTT protocols used. This documentation ensures that developers, users, and administrators can easily understand and manage the system.

Step 9: Deployment and Hosting

After the testing phase, the system is deployed by connecting the NodeMCU to the pacemaker and configuring it to send data continuously to the ThingSpeak server. The ThingSpeak platform acts as the cloud service, where real-time heart rate data is visualized and stored. All security protocols, including SSL encryption for data transmission, are activated to guarantee the protection of patient data at every stage.

Step 10: Training and Support

The final step involves providing training and support to users, including healthcare professionals and system administrators. User manuals and training sessions are offered to explain how to monitor real-time heart rate data, manage device connectivity, and respond to alerts. Support services are also set up to help users with troubleshooting and technical issues.

4. IMPLEMENTATION AND RESULTS

The IoT-based pacemaker monitoring system was designed to continuously track heart rate and SpO2 levels with an emphasis on secure data transmission and real-time analysis. At the core of the system is the MAX30100 sensor, which integrates a pulse oximeter and heart rate sensor for accurate biometric readings. The ESP8266 NodeMCU microcontroller manages sensor communication and processes the data before transmitting it over the internet to the ThingSpeak platform using MQTT. Data encryption, Sensitive health information is shielded from unwanted access through the use of the AES algorithm, in line with the security requirements of the No Zero Thrust Architecture (NZTA).

Figure 1 demonstrates the flowchart of the system's operation, detailing the entire process from data acquisition to secure cloud transmission. The flow begins with the MAX30100 sensor capturing the heart rate and SpO2 data, which is then processed by the NodeMCU. After processing, the ESP8266 encrypts the raw biometric data using AES encryption with a 128-bit key. The encrypted data is then transmitted to ThingSpeak using the MQTT protocol, ensuring secure and reliable delivery. The system operates in a loop where sensor data is updated and sent every 10 seconds. The NZTA's integration offers a safe, resilient channel for data transfer and guarantees that there isn't a single point of failure, adding an extra layer of cybersecurity to the architecture.

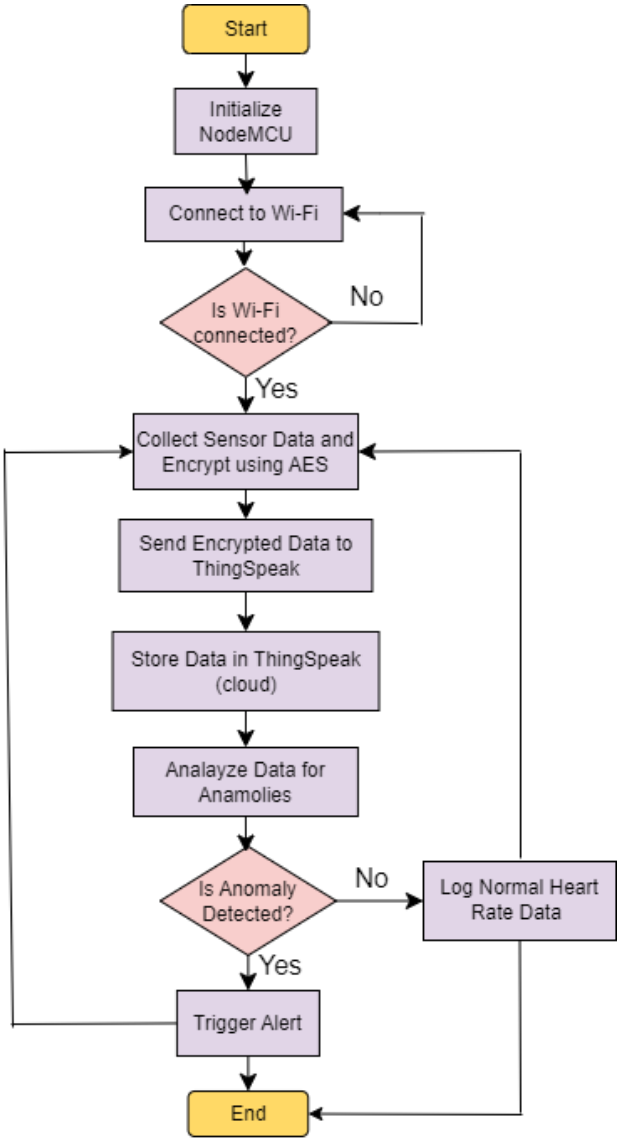


Figure 1. Flowchart

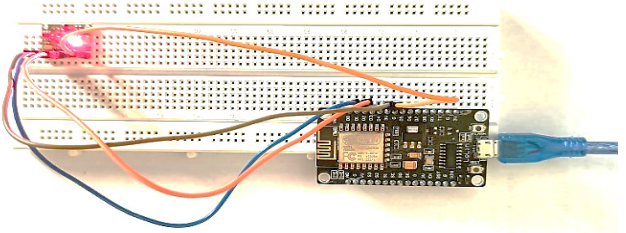
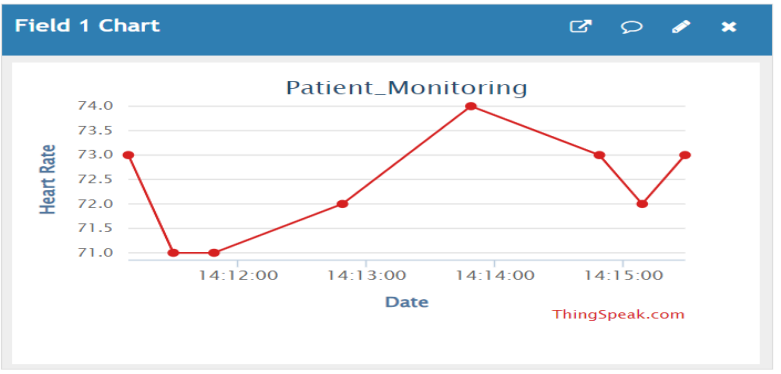


Figure 2. Hardware setup

The hardware setup, illustrated in Figure 2, consists of the MAX30100 sensor connected to the NodeMCU ESP8266, which handles the data acquisition and communication processes. The compact design of the system allows for real-time biometric monitoring without the need for complex, bulky equipment. The MAX30100 sensor module, with its infrared and red LEDs, measures heart rate and blood oxygen levels non-invasively. The NodeMCU, connected via Wi-Fi, is responsible for encrypting and transmitting the data securely over the internet. This minimalistic hardware setup makes the system suitable for both home and clinical environments, offering scalability for future healthcare applications.



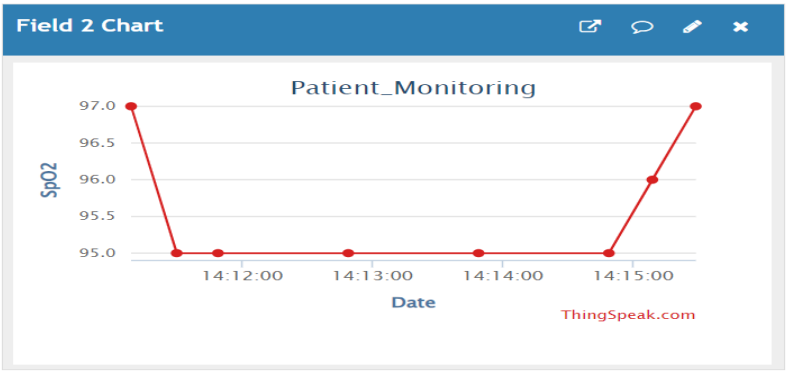


Figure 3. Thingspeak dashboard

The ThingSpeak platform is used as the cloud service for data storage and visualization. Once the encrypted data is transmitted from the ESP8266, ThingSpeak's MQTT broker receives and decrypts the data for analysis and visualization. Figure 3 shows the heart rate and SpO2 levels as plotted graphs on ThingSpeak's dashboard. The data is continuously updated and presented in real time, allowing medical professionals or caregivers to monitor the patient's vital signs from a remote location. The ThingSpeak channel is configured to plot the heart rate on one field and SpO2 on another, enabling clear and distinct monitoring of both parameters. By using ThingSpeak, the system benefits from robust data logging capabilities and seamless integration with other IoT platforms.

Security is a critical component of this system, and AES encryption was employed to ensure the confidentiality of the transmitted health data. Sensitive health information is shielded from unwanted access through the use of the AES algorithm.prior to the data being transmitted to Thingspeak over MQTT, the ESP8266 encrypts it. We make sure that even if the data is intercepted during transmission, it cannot be decoded without the proper AES key and initialisation vector by encrypting the heart rate and SpO2 readings (IV). This encrypted data stream complies with modern healthcare standards and aligns with NZTA's goal of establishing a secure, zero-compromise transmission pipeline. The NZTA framework ensures that no unsecured data is transmitted, which is crucial in healthcare scenarios where patient data security is of paramount importance.

Figure 4 illustrates the custom-developed web dashboard that displays the patient's heart rate and SpO2 levels. This webpage retrieves data directly from ThingSpeak's cloud platform and presents it in a user-friendly format. The webpage provides real-time

updates of the patient's biometric data, ensuring that healthcare providers or family members can immediately react if any abnormal heart rate or oxygen saturation levels are detected. By leveraging MQTT and ThingSpeak's visualization tools, the system ensures that the data is not only secure but also easily accessible and interpretable for end users. The web interface was designed with simplicity and efficiency in mind, offering an intuitive display of critical health metrics without requiring complex software or hardware configurations.

In summary, the implementation of this pacemaker monitoring system successfully combines biometric sensing, secure communication, and real-time cloud-based visualization. The integration of MAX30100 with NodeMCU ESP8266, AES encryption, MQTT protocol, and ThingSpeak provides a comprehensive solution for secure remote monitoring of vital health parameters. The use of NZTA ensures a secure, fault-tolerant architecture that safeguards patient data throughout the transmission process. The system's flexibility, security, and scalability make it a viable solution for healthcare applications, particularly in monitoring pacemaker patients where continuous and secure access to biometric data is essential.

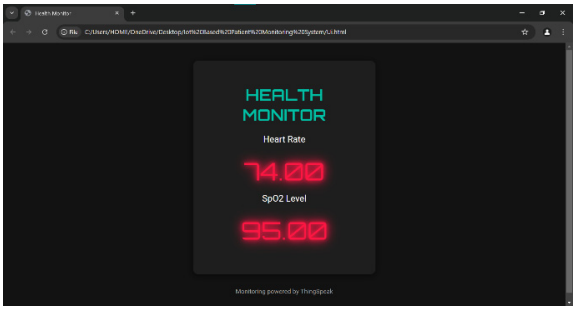


Figure 4. Custom-made web interface

5. CONCLUSION

The IoT-based pacemaker monitoring system developed in this project effectively demonstrates the use of modern technology to securely track important health indicators in real time, like heart rate and SpO2 levels. By integrating the MAX30100 sensor with the NodeMCU ESP8266 microcontroller and utilizing the ThingSpeak platform, the system provides continuous health monitoring with cloud-based visualization. The use of MQTT protocol ensures efficient data transmission, while AES encryption provides a

crucial layer of security, shielding private patient data from possible online attacks. The incorporation of the No Zero Thrust Architecture (NZTA) further strengthens the system's security by ensuring fault-tolerant and secure transmission paths, making the system highly resilient to breaches.

Overall, the project highlights the potential of IoT in healthcare, offering a scalable and adaptable solution that can be expanded to monitor additional vital signs. The real-time monitoring capabilities, combined with secure data handling, empower healthcare providers with immediate access to patient data, improving response times and enhancing patient safety. This method offers a promising way to raise the standard of care and lower the risk of serious health problems by laying the groundwork for future advancements in safe, remote health monitoring.

REFERENCES

1. M. H. D. Mohamed, R. Mukhtar, and M. H. R. Rizvi. "Design and Development of an IoT-Based Patient Health Monitoring System." International Journal of Engineering and Technology, vol. 7, no. 2, pp. 1-5, 2018.
2. D. G. Owais, and A. B. R. Kalra. "Healthcare Security in IoT: Challenges and Solutions." IEEE Transactions on Network and Service Management. vol. 16, no. 4, pp. 1546-1561, 2019.
3. F. Alzahrani, R. G. N. Almashaan, and Y. E. S. Alsolami. "A Cloud-Based IoT Framework for Remote Patient Monitoring." Sensors, vol. 20, no. 12, 2020. DOI: 10.3390/s20123360.
4. J. B. Rao and P. K. Gupta. "Cybersecurity for Medical Devices: Protecting the Patient's Data." Journal of Medical Systems, vol. 42, no. 10, 2018. DOI: 10.1007/s10916-018-1060-6.
5. K. F. M. N. M. Mohamad, K. M. Kamarudin, and A. N. Yusof. "Design and Implementation of Heart Rate Monitoring System Using IoT." International Journal of Emerging Trends in Engineering Research, vol. 8, no. 3, pp. 1394-1398, 2020.
6. A. Shafique, S. Z. A. Hussain, and M. U. A. Khan. "Blockchain Technology for Secure Data Sharing in IoT-Based Healthcare Systems." IEEE Access, vol. 9, pp. 29073-29086, 2021. DOI: 10.1109/ACCESS.2021.3055130.
7. R. Ahmad and I. Ahmad. "IoT-Based Health Monitoring System with Patient Feedback Mechanism." International Journal of Computer Applications, vol. 975, no. 8887, 2018.
8. T. Alam, F. Hossain, and M. Rahman. "IoT-Based Smart Health Care System." Proceedings of the International Conference on Electrical, Computer, and Communication Engineering, 2020.
9. H. A. A. Abokhodair, A. A. Alotaibi, and A. A. Aldayel. "Using IoT Devices for Blood Pressure Monitoring." Journal of Network and Computer Applications, vol. 102, pp. 51-63, 2018. DOI: 10.1016/j.jnca.2018.05.001.
10. S. M. K. Nazari and E. J. Dunne. "Heart Rate Monitoring Using IoT: An Application in Cardiac Health." Journal of Medical Engineering, 2021. DOI: 10.1155/2021/6615879.

11. M. Patel, R. K. Awasthi, and J. S. Mehta. "Cybersecurity Issues in the Internet of Things (IoT): A Survey." Future Generation Computer Systems, vol. 109, pp. 136-153, 2020. DOI: 10.1016/j.future.2020.02.025.
12. M. I. Niranjana, J. Dhanasekar, S. Karan, N. N. Kumar, C. B. Mithul and S. P. Kumar, "Solar Tree based Home Appliance Monitoring System using IoT," *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, Coimbatore, India, 2023, pp. 1374-1379, doi: 10.1109/ICECA58529.2023.10395400.
13. A. G. S. Meena, B. S. K. M. K. Kumaran, and M. R. A. V. N. Iyer. "Security Framework for IoT-Enabled Health Monitoring Systems." Healthcare Technology Letters, vol. 6, no. 1, pp. 16-22, 2019. DOI: 10.1049/htl.2018.5015.
14. C. N. Abubakar, S. M. Farhan, and T. S. Khokhar. "Design of Smart Health Monitoring System Using IoT." International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 11, pp. 2612-2616, 2019.
15. M. I. Niranjana, V. Parthipan, J. Dhanasekar, M. Jesheer, M. G. Giridaran and K. L. Harishankar, "An Innovative IoT Based Surveillance Robot for Smart Applications," *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, Coimbatore, India, 2023, pp. 377-382, doi: 10.1109/ICECA58529.2023.10395527.
16. K. U. A. Naqvi and A. Ali. "IoT in Healthcare: Challenges, Opportunities, and Solutions." Health Information Science and Systems, vol. 7, no. 1, 2020. DOI: 10.1007/s13755-020-00304-3.
17. V. K. V. A. Kumar and M. K. S. Singh. "IoT Based Health Monitoring System Using Heartbeat Sensor." Journal of Medical Systems, vol. 44, no. 9, 2020. DOI: 10.1007/s10916-020-01616-4.
18. D. A. Patil and M. V. Kumavat. "Implementing Cyber Security in IoT for Healthcare." International Journal of Advanced Research in Computer Science and Software Engineering, vol. 9, no. 4, pp. 123-129, 2019.
19. S. Gupta and M. K. Sharma. "A Comprehensive Review of Security in IoT-Based Healthcare Systems." Journal of Health Engineering, 2021. DOI: 10.1155/2021/5514023.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.