WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Zero Trust Architecture for Secure IoT-Enabled Medical Device Networks

Devanshu Chauhan[1], Sakshi Joshi[2] and Vishesh P. Gaikwad[3]

[1]Department of Computer Science and Engineering, Sardar Vallabhbhai National Institute of Tech- nology, Surat, Gujarat, India, e-mail: devanshuchauhan54321@gmail.com

[2]Department of Computer Science and Engineering, Sardar Vallabhbhai National Institute of Tech- nology, Surat, Gujarat, India, e-mail: sakshi12joshi11@gmail.com

[3]Department of Computer Science and Engineering, Sardar Vallabhbhai National Institute of Tech- nology, Surat, Gujarat, India e-mail: vgaikwad@coed.svnit.ac.in

ABSTRACT

The rapid adoption of the Internet of Things (IoT) in healthcare has led to significant advancements in patient monitoring and medical data acquisition. How- ever, the integration of resource-constrained medical devices into critical health- care infrastructure has also exposed these systems to new security vulnerabilities. Traditional perimeter-based security models are insufficient to safeguard the con- fidentiality, integrity, and availability of sensitive medical data in such distributed environments. This paper presents a practical implementation of a Zero Trust Ar- chitecture (ZTA) tailored for IoT-enabled medical device networks to address these challenges. Leveraging OpenZiti as the core enabler of ZTA principles, the proposed system enforces strict identity-based access control, mutual TLS (mTLS) for secure communication, and robust data encryption using AES-256. The experimental setup includes a Raspberry Pi 5-based IoT gateway integrated with medical sensors such as the MAX30100 pulse oximeter, MPS20N0040D pressure sensor, and MCP3008 analog-to-digital converter. Role-Based and Identity-Based Access Control (RBAC and IBAC) mechanisms are applied to restrict access based on device identities and user roles. Sensor data is securely transmitted to the ThinkSpeak cloud platform for real-time monitoring and visualization. The proposed approach demonstrates a scalable, secure, and practical solution for protecting medical IoT networks against modern cyber threats, paving the way for secure healthcare IoT deployments.

Key words: Zero Trust Architecture, Internet of Medical Things, OpenZiti, Edge Security, IoT Security, Healthcare, mTLS, JWT, RBAC

1. Introduction

The integration of Internet of Things (IoT) technologies into the healthcare sector has transformed the landscape of medical monitoring, diagnostics, and treatment. IoT-enabled medical devices, including physiological sensors and wearable moni- toring systems, facilitate real-time patient health data collection, remote consulta- tions, and proactive healthcare management [11, 15]. These advancements play a critical role in managing chronic illnesses, post-operative care, and elderly health monitoring, providing continuous insights that enhance patient outcomes and opti- mize healthcare resources.

Despite remarkable benefits, the proliferation of IoT in healthcare introduces significant security and privacy concerns. Medical IoT devices often operate in resource-constrained environments, lack standardized security protocols, and com- municate over potentially insecure networks. Moreover, the sensitive nature of health data and the life-critical functionality of many medical devices make them prime targets for cyber attacks, including unauthorized access, data manipulation, and service disruption [7, 19].

Traditional perimeter-based security models are fundamentally insufficient for addressing these risks. Such models assume implicit trust for devices and users within the network boundary, focusing defenses primarily at the network edge. However, the dynamic, distributed, and heterogeneous nature of modern IoT health- care ecosystems renders this perimeter almost obsolete. With mobile devices, cloud platforms, third-party services, and remote access points now commonplace, attack- ers can exploit vulnerabilities from both within and outside the network [9, 4].

In response to these challenges, the Zero Trust Architecture (ZTA) paradigm has emerged as a robust, identity-centric security model designed to eliminate implicit trust within networks. ZTA operates on the principle of "never trust, always verify," enforcing continuous authentication, strict access control, and comprehensive data encryption for every device, user, and service interaction [18, 9, 10]. In recent years, ZTA has been explored in various domains, including industrial IoT [1, 3], health- care information systems [2], and critical infrastructure protection, highlighting its potential to secure complex, distributed systems.

However, while the theoretical benefits of ZTA for healthcare IoT are well- recognized, practical, end-to-end implementations remain scarce. Many existing studies focus on high-level frameworks, simulations, or partial security mechanisms without addressing the complexities of integrating real-world medical devices, en- forcing identity-based access control, and ensuring secure data transmission across the entire system.

This paper presents a comprehensive, practical implementation of a secure IoT-enabled healthcare monitoring system based on ZTA principles. Leveraging OpenZiti, an open-source software-defined networking (SDN) platform designed for enforcing identity-based, secure overlay networks, the proposed system in- tegrates widely used medical sensors—including the MAX30100 pulse oxime- ter, MPS20N0040D pressure sensor, and MCP3008 analog-to-digital converter (ADC)—with a Raspberry Pi 5-based IoT gateway.

To ensure end-to-end security, the system incorporates mutual Transport Layer Security (mTLS) for device and network authentication, Role-Based Access Con- trol (RBAC) and Identity-Based Access Control (IBAC) for granular permission enforcement, JSON Web Tokens (JWT) for secure session management, and Ad- vanced Encryption Standard (AES-256) for data protection. Furthermore, the medi- cal data is securely transmitted to ThinkSpeak, a cloud-based platform for real-time visualization and monitoring, enabling healthcare providers to access critical health information while preserving security and privacy.

The major contributions of this work are as follows:

- Design and implementation of a ZTA-based, secure medical IoT architecture us- ing OpenZiti.
- Practical integration of medical sensors with a Raspberry Pi 5 IoT gateway and secure overlay network.
- Application of mTLS, RBAC, IBAC, JWT, and AES-256 to enforce authentica- tion, access control, and data encryption.
- Real-time, secure transmission and visualization of medical data using the ThinkS- peak cloud platform.
- Experimental validation demonstrating the system's ability to mitigate common security threats in medical IoT environments.

2. Related Work

The increasing integration of Internet of Things (IoT) technologies into health- care infrastructures has simultaneously enhanced patient monitoring capabilities and introduced significant security challenges. The inherently distributed, resource- constrained, and heterogeneous nature of medical IoT devices makes them vulner- able to a wide range of cyber threats, necessitating advanced security frameworks beyond traditional perimeter-based models.

The concept of Zero Trust Architecture (ZTA), introduced by Kindervag [18], fundamentally redefined network security by eliminating implicit trust and enforc- ing strict verification mechanisms for all devices, users, and services, irrespective of their network location. Stafford [9] further formalized ZTA principles through the NIST SP 800-207 standard, providing a structured approach for implementing Zero Trust across diverse systems, including cloud environments and IoT networks.

Syed et al. [10] presented a comprehensive survey of ZTA, highlighting its appli- cability to modern networks and outlining key challenges, such as identity manage- ment, access control, and secure data transmission, particularly in IoT ecosystems. He et al. [8] expanded upon this by identifying open research issues related to ZTA implementation in dynamic, resource-limited environments like healthcare IoT.

In the context of Industrial IoT (IIoT), Federici et al. [1] and Zanasi et al. [3] demonstrated how ZTA can be applied to secure remote access and critical infras- tructure, showcasing the need for flexible, identity-driven security mechanisms. Li et al. [4] explored future IoT architectures integrated with Zero Trust, emphasizing their role in safeguarding distributed industrial networks.

The healthcare domain presents unique challenges due to the criticality of med- ical data and device functionality. Edo et al. [2] proposed incorporating ZTA prin- ciples into Health Information Systems (HIS) to enhance data confidentiality and integrity. Angle [**?**] and Kaluza [19] discussed the necessity of applying ZTA specif- ically to medical device ecosystems, highlighting the severe risks posed by unautho- rized access and device manipulation.

Liu et al. [6] provided an extensive review of ZTA's implementation in IoT envi- ronments, identifying technical gaps such as lightweight cryptographic mechanisms and scalable identity verification suitable for constrained devices. Vakhter et al. [7] focused on threat modeling for wireless biomedical devices, underscoring their sus- ceptibility to cyberattacks and reinforcing the importance of robust, end-to-end se- curity solutions.

Several studies have explored IoT and cloud integration in healthcare, yet they often lack practical, fully implemented solutions that combine ZTA with medical IoT. Works such as [11, 15, 14] discuss IoT system architectures and security chal- lenges in general terms, while Udayakumar and Anandan [12] and Murthy et al.

[17] detail cloud-based IoT security but without explicit ZTA integration.

Despite significant research progress, a notable gap exists in the practical deploy- ment of complete ZTA-enabled medical IoT systems that address device authenti- cation, access control, secure communication, and real-time data monitoring in an integrated manner. Existing works largely focus on conceptual frameworks, theo- retical models, or isolated security features, leaving the real-world complexities of healthcare IoT integration underexplored.

To address these limitations, this work presents a comprehensive, fully im- plemented ZTA-enabled IoT medical monitoring system. It combines OpenZiti's software-defined, identity-centric security architecture with real-world medical sen- sors, a Raspberry Pi 5-based gateway, advanced

encryption, and secure cloud-based visualization. This practical implementation demonstrates the feasibility of deploy- ing ZTA principles effectively in healthcare IoT environments, ensuring end-to-end security, robust access control, and reliable medical data transmission.

3. Architecture

The system presents a secure, Zero Trust Architecture (ZTA)-enabled IoT healthcare monitoring framework that ensures end-to-end protection of sensitive medical data and device integrity. The design leverages the principles of identity-centric access control, encrypted communication, and continuous authentication, tailored specifi- cally for resource-constrained medical IoT environments.

3.1 System Overview

The system architecture, illustrated in Fig. 1, comprises the following key compo- nents:

- **Medical Sensors:** The physiological parameters of patients are acquired using a combination of widely used medical sensors. The MAX30100 pulse oximeter monitors heart rate and oxygen saturation, the MPS20N0040D pressure sensor facilitates pressure monitoring (e.g., blood pressure), and the MCP3008 analog- to-digital converter (ADC) enables seamless interfacing of analog medical sen- sors with the digital platform.
- **IoT Gateway (Raspberry Pi 5):** Acting as a local processing and communi- cation hub, the Raspberry Pi 5 aggregates sensor data, enforces security poli- cies, and establishes a secure, identity-bound connection with the overlay net- work. OpenZiti is deployed on the gateway to provide software-defined, ZTA- compliant connectivity.
- **OpenZiti Edge Router:** Positioned within the network perimeter, the Edge Router functions as a ZTA-enforced gateway that facilitates secure tunneling of data to authorized destinations. It authenticates device identities, enforces access policies, and ensures that only verified entities participate in the network.
- **Secure Cloud Platform (ThinkSpeak):** Medical data is transmitted to ThinkS- peak, a secure cloud-based platform for real-time data visualization and monitor- ing. The platform allows authorized healthcare providers to access patient health metrics while ensuring data confidentiality and integrity.
- **Authorized Users:** Users such as doctors, nurses, or administrative staff access the system based on Role-Based Access Control (RBAC) and Identity-Based Ac- cess Control (IBAC) policies, ensuring that only authenticated individuals with appropriate privileges can view or manage patient data.

3.2 Security Mechanisms

The system integrates multiple layers of security, adhering to Zero Trust principles:

- **Mutual TLS (mTLS):** All communications between the sensors, gateway, and cloud platform are secured using mutual Transport Layer Security, ensuring de- vice authentication and encrypted data transmission.
- **RBAC and IBAC:** Access control is enforced both at the role and identity levels. Each device and user is assigned specific identities, and access is granted strictly based on predefined policies managed within OpenZiti.
- **JWT-based Session Security:** JSON Web Tokens (JWT) are employed to man- age authenticated sessions, preventing session hijacking and unauthorized access.

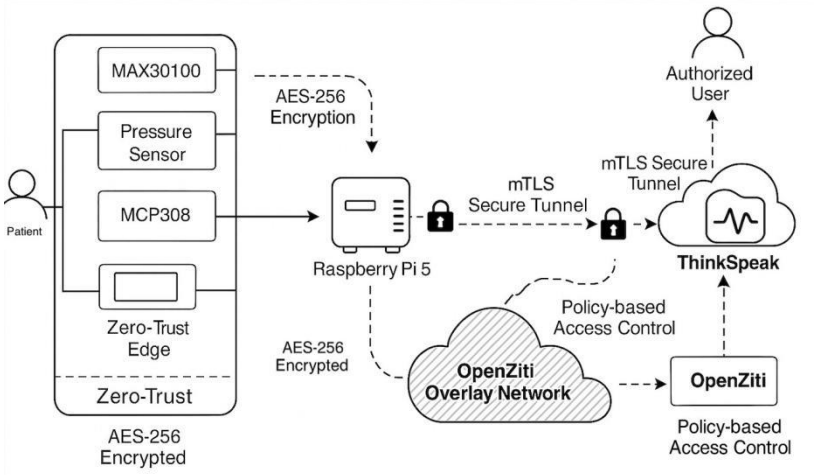

Fig. 1 Proposed ZTA-enabled Secure IoT Healthcare Architecture.

- **Data Encryption (AES-256):** Sensor data is encrypted using Advanced Encryp- tion Standard (AES-256) before transmission, safeguarding sensitive health in- formation from eavesdropping or tampering.
- **Continuous Monitoring:** The system continuously monitors device status, con- nection integrity, and user access patterns to detect anomalies or potential secu- rity breaches in real time.

3.3 Identity Management

Every system component, including medical sensors and the IoT gateway, is en- rolled as a distinct identity within the OpenZiti controller. This identity-centric ap- proach ensures that only verified entities can participate in the network, effectively mitigating risks associated with unauthorized devices or rogue actors.

3.4 Data Flow

The secure data flow within the system proceeds as follows:

1. Medical sensors acquire physiological data and transmit it to the Raspberry Pi 5 via wired interfaces.
2. The IoT gateway authenticates with the OpenZiti overlay network and securely forwards encrypted sensor data.
3. The OpenZiti Edge Router verifies identities and enforces access policies, allow- ing only authorized traffic through.
4. The data is transmitted securely to the ThinkSpeak cloud platform.
5. Authorized users access real-time medical data through secure, policy-enforced channels.

This layered, identity-driven architecture ensures comprehensive protection for sensitive medical data, device communications, and user interactions, aligning with Zero Trust principles while remaining suitable for resource-constrained IoT health- care deployments.

4. Implementation

The proposed Zero Trust-enabled IoT healthcare monitoring system was fully im- plemented and tested to validate its practical feasibility and security effectiveness. The implementation involves the integration of hardware components, secure soft- ware stack deployment, and configuration of identity-based access controls.

4.1 Hardware Setup

The physical setup of the system comprises the following components:

- **Raspberry Pi 5:** Serving as the IoT gateway, the Raspberry Pi 5 provides ad- equate computational resources to interface with medical sensors, run security services, and maintain secure network communication.
- **Medical Sensors:**
  - **MAX30100 Pulse Oximeter:** Measures heart rate and blood oxygen satura- tion (SpO_2) levels.
  - **MPS20N0040D Pressure Sensor:** Facilitates pressure-based physiological measurements, including potential blood pressure monitoring.
  - **MCP3008 ADC:** An 8-channel analog-to-digital converter that interfaces analog medical sensors with the Raspberry Pi's digital GPIO pins.
- **OpenZiti Edge Router:** Deployed within the network, the Edge Router provides identity-bound, secure tunneling of data between the IoT gateway and the cloud platform.

A fully wired connection was established between the medical sensors and the Raspberry Pi using a breadboard and jumper wires to ensure signal integrity and system stability during testing.

4.2 Software Stack

The software stack was carefully configured to enforce Zero Trust security princi- ples across all system layers:

- **Operating System:** Raspberry Pi OS (64-bit) was installed on the Raspberry Pi 5 to provide a stable Linux-based environment.

- **Sensor Interfacing:** Python scripts were developed to acquire data from the MAX30100 and MPS20N0040D sensors. The MCP3008 ADC was interfaced using the spidev library to digitize analog sensor readings.
- **OpenZiti Setup:**
  - The OpenZiti controller was configured on a secure system to manage net- work identities and access policies.
  - The Raspberry Pi was enrolled as an authenticated identity within the Open- Ziti network using the ziti edge enroll process.
  - An OpenZiti Edge Router was deployed to enforce secure, identity-bound data tunneling.
- **Security Features:**
  - **mTLS:** Mutual authentication between the Raspberry Pi, Edge Router, and OpenZiti controller was implemented using mTLS certificates.
  - **RBAC and IBAC:** Access policies were configured within OpenZiti to re- strict device and user permissions based on roles and unique identities.
  - **JWT:** JSON Web Tokens were utilized for authenticated session management.
  - **AES-256 Encryption:** Sensor data was encrypted using AES-256 before transmission to the cloud platform.
- **Cloud Integration:** The ThinkSpeak platform was configured to receive en- crypted sensor data from the Raspberry Pi via secure tunnels. Real-time data visualization dashboards were created for authorized healthcare providers.

4.3 Identity Enrollment and Access Control

Each system component was assigned a unique identity within the OpenZiti con- troller. The following entities were enrolled:

- MAX30100 Sensor
- MPS20N0040D Sensor
- MCP3008 ADC Interface
- Raspberry Pi 5 IoT Gateway
- Edge Router

Role-based permissions were assigned to human users (e.g., patient, nurse, staff), while identity-based policies ensured that only enrolled devices could transmit or access data within the system

4.4 Data Transmission Flow

The implemented data flow follows the architecture outlined in Section 3:

1. Sensor data is continuously acquired by the Raspberry Pi through GPIO and SPI interfaces.
2. The data is encrypted locally using AES-256.
3. The Raspberry Pi establishes a secure tunnel to the OpenZiti Edge Router, au- thenticated via mTLS.
4. The Edge Router verifies device identity and enforces access policies.
5. Data is securely forwarded to ThinkSpeak for visualization.
6. Authorized users access real-time patient data through role- and identity-enforced channels.

4.5 System Validation

The complete system was deployed and validated under controlled conditions. Func- tionality tests confirmed:

- Successful identity-based device enrollment and authentication.
- Enforced access control preventing unauthorized data transmission or access.
- Secure, encrypted data transmission through OpenZiti overlay networks.

This practical, end-to-end implementation demonstrates the feasibility of apply- ing ZTA principles to secure medical IoT deployments.

5. Results and Security Analysis

The proposed Zero Trust-enabled IoT healthcare monitoring system was rigorously tested to evaluate its functional performance, security effectiveness, and practical feasibility. The results validate the system's capability to provide secure, real-time health data monitoring while mitigating common IoT security threats.

5.1 Functional Validation

The system was deployed in a controlled environment with simulated patient health parameters. The following functional aspects were verified:

- **Sensor Data Acquisition:**
  - The MAX30100 sensor successfully measured heart rate and blood oxygen saturation (SpO_2).
  - The MPS20N0040D pressure sensor reliably captured pressure values.
  - The MCP3008 ADC accurately digitized analog sensor data for processing.
- **Real-Time Data Transmission:** Encrypted sensor data was transmitted from the Raspberry Pi 5 to the ThinkSpeak cloud platform via secure OpenZiti tunnels, with no observed data loss or transmission delay under normal network condi- tions.
- **Data Visualization:** Real-time graphs for SpO_2, heart rate, and pressure were generated on ThinkSpeak, accessible only to authorized users based on enforced access policies.

6. Conclusion and Future Work

This paper presented a fully implemented Zero Trust Architecture (ZTA)-enabled IoT healthcare monitoring system designed to ensure the security, privacy, and integrity of patient data in resource-constrained environments. By leveraging OpenZiti's identity-based overlay network, mutual TLS, AES-256 encryption, and strict RBAC/IBAC policies, the system effectively addresses common secu- rity threats in medical IoT deployments. The integration of sensors like MAX30100 and MPS20N0040D with a Raspberry Pi 5 gateway allowed for reliable physio- logical data acquisition and real-time visualization on ThinkSpeak.

The system was validated in a controlled setup and demonstrated strong re- silience to unauthorized access, data breaches, and network-level attacks. Per- formance metrics indicated minimal latency and efficient resource utilization, supporting the feasibility of deploying ZTA in real-world healthcare scenarios. The modular and scalable design also enables the integration of additional sen- sors or services without compromising security.

Future Work

Despite its robustness, several areas for enhancement remain:

- **Scalability Testing:** Future work includes scaling the system for large-scale hospital environments involving dozens of sensors and multiple gateways, with performance benchmarking under high data volume.
- **AI-based Anomaly Detection:** Incorporating machine learning techniques for real-time anomaly detection in physiological readings and device behavior will strengthen proactive threat mitigation.
- **Compliance Integration:** Future iterations will explore integration with health- care regulatory standards such as HIPAA or HL7 FHIR to support secure in- teroperability with Electronic Health Record (EHR) systems.
- **Hardware Security Modules (HSM):** Integration of HSMs or Trusted Plat- form Modules (TPMs) on gateways for key storage will further harden the cryptographic infrastructure.
- **Offline Capabilities:** Introducing secure offline data buffering and synchro- nization mechanisms can improve system robustness in unstable network con- ditions.

The project confirms that ZTA is not only applicable but highly effective in se- curing next-generation medical IoT infrastructures. This lays the foundation for future research into secure, scalable, and compliant digital healthcare ecosys- tems.

References

1. F. Federici, D. Martintoni, and V. Senni, "A zero-trust architecture for remote access in industrial IoT infrastructures," *Electronics*, vol. 12, no. 3, p. 566, 2023.
2. O. C. Edo, D. Ang, P. Billakota, and J. C. Ho, "A zero trust architecture for health infor- mation systems," *Health and Technology*, vol. 14, no. 1, pp. 189–199, 2024.

3. C. Zanasi, S. Russo, and M. Colajanni, "Flexible zero trust architecture for the cybersecu- rity of industrial IoT infrastructures," *Ad Hoc Networks*, vol. 156, p. 103414, 2024.
4. S. Li, M. Iqbal, and N. Saxena, "Future industry internet of things with zero-trust security," *Information Systems Frontiers*, pp. 1–14, 2022.
5. Alex Kaluza, "Medical Devices in a Zero Trust Architecture," *ISSA Journal*, vol. 21, no. 4, 2023.
6. C. Liu *et al.*, "Dissecting zero trust: research landscape and its implementation in IoT," *Cybersecurity*, vol. 7, no. 1, p. 20, 2024.
7. V. Vakhter, B. Soysal, P. Schaumont, and U. Guler, "Threat modeling and risk analysis for miniaturized wireless biomedical devices," *IEEE Internet of Things Journal*, vol. 9, no. 15, pp. 13338–13352, 2022.
8. Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A survey on zero trust architecture: Chal- lenges and future trends," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 6476274.
9. V. Stafford, "Zero trust architecture," *NIST Special Publication*, vol. 800, no. 207, 2020.
10. N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero trust archi- tecture (ZTA): A comprehensive survey," *IEEE Access*, vol. 10, pp. 57143–57179, 2022.
11. P. R. Gunjal, S. R. Jondhale, J. L. Mauri, and K. Agrawal, *Internet of Things: Theory to Practice*, CRC Press, 2024.
12. P. Udayakumar and R. Anandan, *Design and Deploy IoT Network & Security with Mi- crosoft Azure*, Springer, [Year unspecified].
13. P. D. Singh and M. Angurala, *Integration of Cloud Computing and IoT: Trends, Case Studies and Applications*, CRC Press, 2024.
14. A. Kumar, A. Prasad, and T. P. Singh, "Communication technologies and security chal- lenges in IoT: An introduction," in *Communication Technologies and Security Challenges in IoT*, Springer Nature Singapore, pp. 1–20, 2024.
15. K. Srivastav, P. Das, and A. K. Srivastava, "Introduction to biotechnology and IoT integration," in *Biotech and IoT: An Introduction Using Cloud-Driven Labs*, Springer, pp. 1–24, 2024.
16. Kadhar and G. Arnand, *Data Science with Raspberry Pi*, Springer, 2021.
17. J. S. Murthy, G. M. Siddesh, and K. G. Srinivasa, *Cloud Security: Concepts, Applications and Practices*, CRC Press, 2024.
18. J. Kindervag, "Build security into your network's DNA: The zero trust network architec- ture," *Forrester Research Inc.*, vol. 27, pp. 1–16, 2010.
19. A. Kaluza, "Medical devices in a zero trust architecture," *ISSA Journal*, vol. 21, no. 4, 2023.