International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0207

e ISSN: 2584-2854
Volume: 02
Issue: 05 May 2024
Page No: 1530-1535

Optimizing Security for Remote Patient Monitoring with Edge Computing Strategies

Mukesh Kumar

Assistant Professor, Computer Science, St. Xavier's College of Management & Technology, Patna, Bihar, India.

Email Id: *mukeshkumar@sxcpatna.edu.in*

Orcid ID: *https://orcid.org/0009-0005-3983-0786*

Abstract

Remote Patient Monitoring (RPM) is a healthcare technology that allows healthcare providers to monitor patients' health remotely using various medical devices and communication technologies. IoT facilitates the integration of diverse medical devices and sensors into a cohesive RPM system. The collected data is transmitted in real-time to healthcare providers or data collection centres where it is analysed and interpreted. During the COVID-19, healthcare facilities faced immense pressure to accommodate a surge in patients. RPM offered a way to monitor and manage non-critical patients remotely, and reduces the risk of exposure to infectious diseases, for both patients and healthcare providers. The traditional approach of data collection was cloud-based platform. In recent times, edge computing has emerged as a promising alternative to traditional cloud-centric architectures, offering solutions to their inherent limitations. In this approach, computation and data storage are closer to the data source, and offers lower latency, reduced bandwidth consumption, and enhanced privacy and security. However, in practical implementation, several factors must be considered, including the scalability, interoperability, and cost-effectiveness of edge computing solutions. Utilizing the close proximity, decentralized processing, and real-time analytics functionalities of edge computing, it is possible to tackle the security issues inherent in RPM systems while maintaining efficient data transmission and processing. This paper proposes a pioneering method for enhancing security in Remote Patient Monitoring (RPM) by integrating edge computing strategies.

Keywords: *Remote Patient Monitoring (RPM), Internet of Things (Iot), Edge Computing, Data Encryption.*

1. Introduction

In recent years, the healthcare landscape has witnessed a paradigm shift towards remote patient monitoring (RPM) as a means to provide continuous and personalized care outside traditional clinical settings. This transition has been accelerated by advancements in digital health technologies, allowing healthcare providers to remotely monitor patients' vital signs, symptoms, and overall health status in real-time. While RPM offers numerous benefits such as improved patient outcomes, reduced healthcare costs, and enhanced accessibility to care, it also introduces significant security challenges. These security challenges must be addressed to ensure the confidentiality, integrity, and availability of patient data. Patient health data collected by RPM systems are highly sensitive and subject to stringent privacy regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States. Unauthorized access to or disclosure of patient data can lead to serious privacy breaches and legal consequences. Ensuring the integrity of patient data is essential to prevent tampering or unauthorized modification, which could lead to incorrect diagnoses or treatment decisions. RPM systems rely on network connectivity to transmit patient data between remote monitoring devices and healthcare facilities. Securing these networks against various cyber threats, such as eavesdropping, Man-in-the-Middle (MitM) attacks, and Distributed Denial of Service (DDoS) attacks. Also, the wearable sensor system is traditionally connected to the cloud and the data can be retrieved and analysed from the cloud. The cloud service providers are responsible for faster analysis and further propagation of data to the concerned people. However, this is not always possible to get everything on time in the case of cloud services. These platforms are handled by third parties and they are actually providing services to thousands or even millions of customers. The wearable devices may generate tremendous amount of data. According to a report given by the Cisco Global Cloud Index (GCI), the amount of data is growing fast and that's an enormous amount [1]. According to the study, private cloud workloads and compute instances will grow from 84 million in 2016 to 144 million in 2021. Similarly, public cloud workloads and compute instances will grow from 59 million in 2016 to 238 million in 2021, at a CAGR of 32%. The increase in data size will drastically decrease the network performance. In Edge-based or Edge-assisted computing everything related to a patient is not transferred to the central repository. Some processing is done at the edge of the network and then only part of the processed data is sent to the central repository (Figure 1). If something related to a patient needs to be responded to in real-time then that information is directly transferred to the connected hospital or doctor through edge computing. It results in real-time response and the patient's life could be saved [2]. Edge computing offers several advantages for enhancing the security of remote patient monitoring systems:

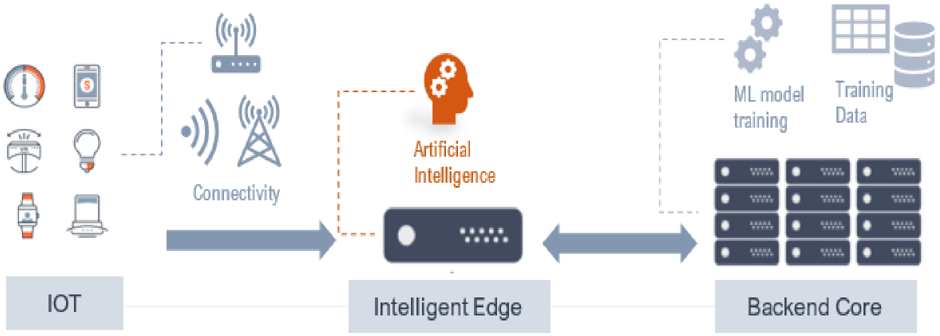

Figure 1 **RPM With Intelligent EDGE**

Proximity to Data Sources: Edge computing nodes are closer to the location where patient data is generated, RPM systems can minimize data transmission over potentially insecure networks, reducing the risk of interception or tampering.

Distributed Processing: Edge computing enables distributed processing of patient data, allowing for real-time analysis and decision-making at the network edge.

Data Encryption and Authentication: Edge computing nodes can implement encryption and authentication mechanisms to secure data both in transit and at rest.

Dynamic Access Control: Edge computing enables dynamic access control policies based on contextual information, such as the location of the data source, the identity of the user, and the sensitivity of the data [3]. In this paper, I have investigated the capabilities of a novel edge computing framework to optimize security for remote patient monitoring by leveraging the proximity, distributed processing, and real-time analytics capabilities of edge computing.

2. Edgex Foundry: An Open-Source Edge Computing Framework for RPM

EdgeX Foundry, an open-source framework, offers the advantage of being freely available, and can run on lightweight hardware and requires minimal resources, making it suitable for edge devices with limited processing power and memory. EdgeX Foundry provides configuration files for each service, allowing you to customize settings according to your requirements. EdgeX Foundry supports various protocols for integrating with IoT devices, including MQTT, Modbus, OPC-UA, and others. It provides data ingestion services such as Core Data and Core Command, which collect, store, and process data from connected devices. Applications can be developed using programming languages such as Java, Python, or Node.js, depending on our preference and the capabilities of the services we are interacting with. EdgeX Foundry provides SDKs and client libraries for interacting with its services programmatically, making it easier to develop custom applications. It is also possible to use artificial intelligence (AI) and machine learning (ML) with EdgeX Foundry to enhance edge computing applications. EdgeX Foundry provides a flexible framework for ingesting data from IoT devices, processing it at the edge, and integrating with various analytics and AI/ML tools. It can preprocess data from IoT devices before sending it to AI/ML models for analysis. Preprocessing may involve cleaning, filtering, or transforming the data to make it suitable for machine learning algorithms. We can deploy AI/ML models directly onto edge devices or on servers located near the edge using frameworks such as TensorFlow Lite, ONNX Runtime, or TensorFlow Serving. EdgeX Foundry allows you to execute AI/ML models at the edge for real-time inference. This enables quick decision-making and reduces the need to send data back to centralized servers for processing. By running inference at the edge, you can reduce latency, bandwidth usage, and reliance on cloud services, making edge deployments more efficient and responsive. This is crucial for health monitoring applications where timely detection and response to health-related events are critical, especially in remote or resource-constrained areas where access to centralized healthcare facilities may be limited (Figure 2). India's vast and diverse population presents unique challenges for healthcare infrastructure. India faces a rising burden of chronic diseases such as diabetes, hypertension, and cardiovascular diseases. EdgeX Foundry's modular and scalable architecture allows for the deployment of health monitoring solutions that can be tailored to different healthcare settings, from urban hospitals to remote rural clinics. EdgeX Foundry offers cost-effective solutions for building and deploying health monitoring applications. This is particularly important in India, where healthcare resources are often limited, and cost constraints can hinder the adoption of advanced medical technologies. EdgeX Foundry can empower India to enhance its healthcare infrastructure and elevate the delivery of healthcare services to its diverse population.

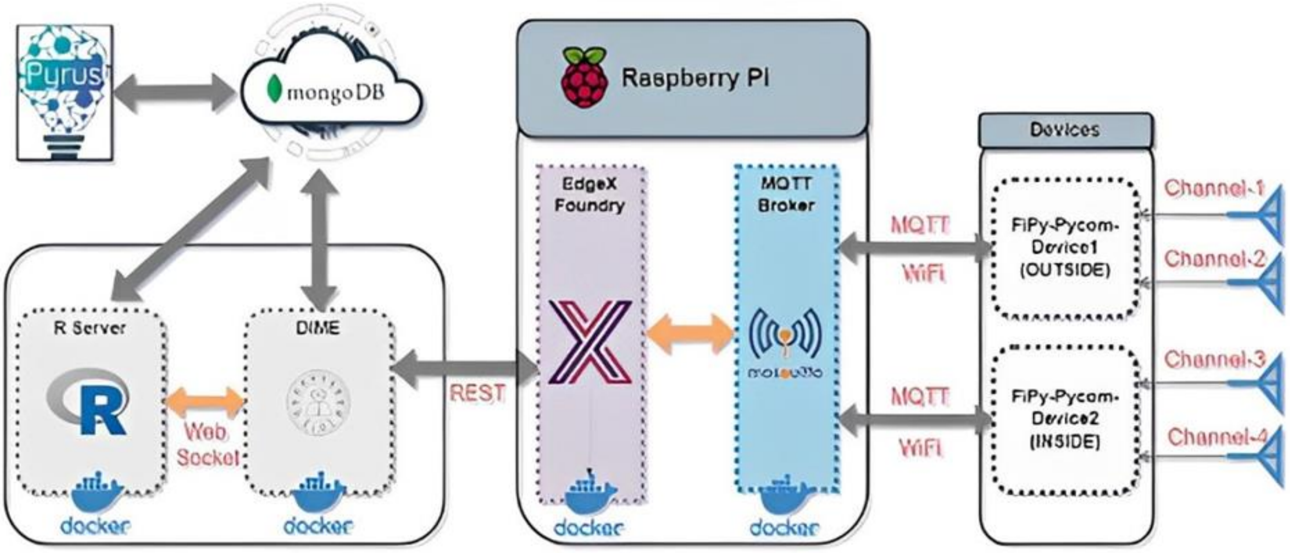

Figure 2 Edgex Foundry For RPM

3. Security Threats and Privacy Attacks in Remote Patient Monitoring

Attackers can inject some software/hardware components to the system and this will enable adversaries such as bypassing authentication, stealing data, reporting false data. Health Monitoring Systems completely rely on data integrity and there is no room for even a very small error in data collection. Some sensitive information of a patient could be revealed and this may be a violation of personal data protection rules of a country [8]. Sometimes, jamming attacks are there in which attackers intentionally flood the network with counterfeit messages to drain communication, computation and/or storage resources. As a result, authorized users will not be able to use the RPM infrastructure. Even if RPM nodes are not transmitting any data, they may reveal critical information. Attackers may also change the training process of machine learning models of Edge based nodes by injecting misleading data sets [9]. Medical records, health insurance details and payment information could all be obtained by hackers. Personal health information leaks are particularly hazardous to individuals because they can lead to identity theft or financial fraud. The healthcare industry is the most targeted industry for data breaches, with over 470 healthcare breaches reported in 2020 [4], exposing over 37.5 million sensitive records. Anthem, one of the largest health insurers in the United States, suffered a cyberattack resulting in the exposure of personal information of approximately 78.8 million individuals, including names, social security numbers, and medical IDs. Anthem will pay a $39.5 million [5] settlement in connection with the state Attorney Generals' investigation. Third parties may gain unauthorized access to private health records in the absence of appropriate safeguards.

3.1. Edge Computing Strategies to Enhance Security and Privacy

EdgeX Foundry can mitigate privacy attacks and prevent security threats by implementing a combination of technical controls, best practices, and organizational policies. Some of the strategies are listed below:

Encryption: Implement end-to-end encryption for data transmission between EdgeX Foundry components, IoT devices, and external systems. This ensures that patient data remains confidential and secure, even if intercepted by attackers during transit.

Access Control: Enforce strict access controls and authentication mechanisms to prevent unauthorized access to EdgeX Foundry components and patient data. Use role-based access control (RBAC) to limit access privileges based on users' roles and responsibilities [10]. Use secure authentication protocols, such as mutual TLS (Transport Layer Security) or OAuth, to authenticate edge devices and ensure that only authorized devices can access patient data.

Data Minimization: Adopt a principle of data minimization, where only necessary patient data is collected, processed, and stored within EdgeX Foundry [11]. Minimizing the amount of sensitive data reduces the potential impact of a privacy breach or security incident.

Data Integrity Checks: Implement data integrity checks, such as digital signatures or checksums, to detect and prevent unauthorized tampering or modification of patient data stored within EdgeX Foundry [12].

Audit Logging: Enable comprehensive audit logging to record all access and activities related to patient data within EdgeX Foundry. Audit logs help detect suspicious behaviour, track user actions, and facilitate forensic investigations in the event of a security incident [13].

Regular Security Assessments: Conduct regular security assessments, penetration testing, and vulnerability scans to identify and remediate security weaknesses in EdgeX Foundry deployments. This proactive approach helps identify and address potential security threats before they can be exploited by attackers [14].

User Training and Awareness: Provide training and awareness programs for employees, developers, and system administrators involved in EdgeX Foundry deployments. Educate them about security best practices, privacy regulations, and the importance of safeguarding patient data.

Compliance with Regulations: Ensure compliance with relevant privacy regulations and standards, such as HIPAA, GDPR, and local data protection laws. Stay informed about regulatory requirements and updates to ensure that EdgeX Foundry deployments meet legal and compliance obligations.

The storage and transmission of personal health information pose the risk of data breaches or unauthorized access, potentially leading to identity theft, medical fraud, or discrimination. Even aggregated health data, when analysed, can reveal intimate details about an individual's health conditions, lifestyle choices, and habits. Unauthorized access to such information can lead to privacy intrusions and potential stigmatization. One notable example of a data leak in India related to health information is the "Aarogya Setu" app incident. The Aarogya Setu app was launched by the Indian government in April 2020 as a contact tracing tool to help contain the spread of COVID-19. In some of the media publications, it was reported that a security vulnerability in the Aarogya Setu app exposed the personal health data of millions of users [6]. The vulnerability allowed attackers to access sensitive user information, including COVID-19 test results, vaccination status, and other personal details. The issue came to light when a French cybersecurity researcher, Robert Baptiste (also known as Elliot Alderson), discovered the vulnerability and shared it on social media. He demonstrated how an attacker could gain unauthorized access to the health data of users. The vulnerability allowed anyone to retrieve data of any Aarogya Setu user without their consent or knowledge. The incident raised concerns about the security and privacy of health-related data in digital health platforms and the potential for unauthorized access or misuse. Therefore, privacy protection is a major issue in Edge-based IoT, and hence effective mechanisms should be implemented to preserve the privacy of users in the EC-assisted IoT environment [7]. Adopting privacy-preserving data analytics techniques, such as differential privacy or homomorphic encryption, enables organizations to derive valuable insights from aggregated data without compromising individual privacy. These techniques allow computations to be performed on encrypted data or perturbed data, preserving privacy while still enabling meaningful analysis. Techniques such as secure multi-party computation (SMPC) or homomorphic encryption allow aggregation of sensitive health data from multiple sources without revealing individual patient information. Employ privacy-preserving machine learning techniques, such as federated learning or differential privacy, to train predictive models at the edge without exposing individual patient data. These techniques allow for collaborative model training across distributed edge devices while preserving the privacy of patient information.

Conclusion

EdgeX Foundry enhances security in remote patient monitoring and other healthcare applications and offers several key advantages. EdgeX Foundry serves as a catalyst for enhancing security in healthcare, offering a robust framework for building secure, interoperable, and scalable solutions that empower healthcare transformation and improve patient outcomes. I would like to highlight following befits provided by the EdgeX Foundry Framework:

Comprehensive Security Framework: EdgeX Foundry provides a robust framework for building secure IoT solutions in healthcare settings. By incorporating encryption, access controls, and data integrity checks, EdgeX Foundry establishes a comprehensive security foundation to protect patient data and ensure confidentiality.

Interoperability and Integration along with Scalability and Flexibility: EdgeX Foundry promotes interoperability among diverse healthcare devices and systems, enabling seamless integration of security features across the entire ecosystem. This interoperability facilitates secure communication, data sharing, and collaboration between healthcare providers, improving the efficiency and effectiveness of patient care. EdgeX Foundry offers scalability and flexibility to adapt security measures to evolving healthcare needs. Whether deploying remote patient monitoring solutions in hospitals, clinics, or home environments, EdgeX Foundry can scale security controls to accommodate varying requirements and environments.

Empowering Healthcare Transformation: By enhancing security with EdgeX Foundry, healthcare organizations can confidently embrace digital transformation initiatives, such as remote patient monitoring, telemedicine, and data-driven analytics. This empowerment enables healthcare providers to deliver more personalized, efficient, and secure care while safeguarding patient privacy and confidentiality.

Through a combination of encryption, secure data aggregation, user authentication, and privacy-preserving techniques, edge-based RPM solutions can safeguard patient information while enabling timely and personalized healthcare delivery. As the healthcare industry continues to embrace digital transformation, prioritizing security in RPM deployments not only enhances patient trust and compliance with regulations but also advances the overall quality and effectiveness of healthcare services. With a commitment to privacy protection and innovative edge computing strategies, healthcare organizations can realize the full potential of remote patient monitoring while ensuring the security and well-being of patients.

References:

[1]. https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report, accessed on 30th April 2024.

[2]. J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, “Data security and privacy-preserving in edge computing paradigm: Survey and open issues,” IEEE Access, vol. 6, pp. 18 209–18 237, 2018.

[3]. Yu, W.; Liang, F.; He, X.; Hatcher, W.G.; Lu, C.; Lin, J.; Yang, X. A Survey on the Edge Computing for the Internet of Things. IEEE Access 2018, 6, 6900–6919.

[4]. https://www.idtheftcenter.org/2020-data-breaches/, Identity Theft Resource Center, "2020 End-of-Year Data Breach Report", accessed on 28th April 2024.

[5]. https://www.fiercehealthcare.com/tech/anthem-to-pay-39m-to-state-ags-to-settle-landmark-2015-data-breach, accessed on 28th April 2024.

[6]. https://www.thequint.com/tech-and-auto/tech-news/aarogya-setu-data-breach-reported-by-shadow-map, accessed on 3rd May 2024.

[7]. https://www.edgexfoundry.org/why-edgex/, accessed on 3rd May 2024.

[8]. Lytras, M.D.; Sarirete, A. Innovation in Health Informatics: A Smart Healthcare Primer; Academic Press: Cambridge, MA, USA, 2020; ISBN 978-0-12-819043-2.

[9]. https://www.indushealthplus.com/health-statistics-of-india.html, accessed on 28th April 2024.

[10]. R. Roman, R. Rios, J. A. Onieva, and J. Lopez, “Immune system for the internet of things using edge technologies,” IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4774–4781, June 2019.

[11]. Y. Lu and L. D. Xu, “Internet of things (IoT) cybersecurity research: A review of current research topics,” IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2103–2115, April 2019.

[12]. S. Chen, Y. Jiang, H. Wen, W. Liu, J. Chen, W. Lei, and A. Xu, “A novel terminal security access method based on edge computing for IoT,” in 2018 International Conference on Networking and Network Applications (NaNA), Oct 2018, pp. 394–398.

[13]. Mosenia and N. K. Jha, “A comprehensive study of security of internet-of-things,” IEEE Transactions on Emerging Topics in Computing, vol. 5, no. 4, pp. 586–602, Oct 2017.

[14]. D. Liu, Z. Yan, W. Ding, and M. Atiquzzaman, “A survey on secure data analytics in edge computing,” IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4946–4967, June 2019.