Secure Authentication Frame Work With Edge Computing For Real Time Patient Health Monitoring InIomt

Mrs. K. Ramya[1], Manojalex G[2], Mohamed Irfan J[3] ,Kathirvalavan G[4] , Prabu A[5]
[1]Assistant professor, Dept of CSE
[2, 3, 4, 5]Dept of CSE
[1, 2, 3, 4, 5] Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamil Nadu, India.

Abstract- *As healthcare increasingly embraces cloud-based technologies, it faces critical issues such as transmission delays and heightened security risks due to centralized data storage. Traditional cloud setups often fall short in delivering real-time patient data and safeguarding sensitive information from unauthorized access. To overcome these challenges, this project presents a Secure Authentication-Based Patient Report Transmission System powered by Edge Computing. By handling and verifying data at local edge nodes—closer to where it originates—the system significantly reduces latency and enables prompt data delivery, which is essential for time-sensitive medical decisions. This decentralized model not only improves processing speed but also enhances the overall efficiency of data management. To ensure robust security, the system incorporates multi-factor authentication (MFA) and role-based access control (RBAC), which together help confirm user identities and limit access based on professional roles. This innovative framework offers a reliable, secure, and fast method for transmitting healthcare data, making it highly effective for critical care environments that demand both speed and privacy.*

Keywords- Edge Computing, Healthcare Data Security, Patient Report Transmission, Multi-Factor Authentication (MFA),Role-Based Access Control (RBAC),Real-Time Data Processing

I. INTRODUCTION

In recent times, the healthcare sector has undergone significant digital transformation, increasingly depending on cloud-based technologies for handling and exchanging patient information. While cloud computing provides advantages such as scalability and centralized management of data, it also brings notable challenges—particularly concerning delays and security vulnerabilities. These limitations become especially problematic in real-time medical scenarios, where even slight transmission delays can hinder urgent clinical decisions. Additionally, the centralized architecture of cloud systems raises the risk of cyberattacks and unauthorized data access, putting patient confidentiality and data accuracy at risk.

To overcome these obstacles, this project introduces a Secure Authentication-Based Patient Healthcare Report Transmission System powered by Edge Computing. Unlike traditional cloud models, edge computing enables data processing to occur closer to where it is generated—at edge devices or nodes. This localized processing significantly reduces the time taken to transmit data, allowing healthcare professionals to retrieve vital patient information more rapidly. As a result, the system supports faster diagnoses and treatments, improving the quality of care in emergency and time-critical environments.Beyond speed, the system places a strong emphasis on protecting patient data. It incorporates advanced authentication techniques, including Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC). MFA strengthens security by requiring users to confirm their identity through multiple verification steps, such as passwords and biometric checks. RBAC, on the other hand, ensures users only have access to data that aligns with their job roles, preventing unnecessary exposure of sensitive information.

By combining edge-based data handling with stringent security protocols, the proposed system addresses the common pitfalls of conventional cloud setups. It delivers a secure, efficient, and scalable method for transmitting healthcare information, making it especially well-suited for high-stakes clinical settings where both speed and privacy are essential.

II. RELATED WORK

The integration of secure authentication frameworks with edge computing for real-time patient health monitoring in the Internet of Medical Things (IoMT) has emerged as a significant area of research in recent years. A growing body of literature highlights the evolution of edge-based architectures designed to support low-latency, high-reliability data

transmission in time-sensitive medical environments. Researchers have explored various methods to safeguard patient data, focusing on authentication techniques such as multi-factor authentication (MFA) and role-based access control (RBAC) to ensure secure access to health records. These studies have laid a strong foundation for developing intelligent, privacy-preserving systems that address both performance and security challenges in real-time healthcare monitoring.

2.1 Cloud-Based Healthcare Data Management

Numerous studies have explored the role of cloud computing in modern healthcare systems, particularly for storing and managing vast amounts of patient data. Traditional cloud infrastructures, while scalable and cost-effective, have shown limitations in real-time data handling due to transmission delays and network dependencies. For instance, researchers have highlighted how centralized cloud systems often struggle to meet the time-sensitive needs of clinical environments, where any latency can negatively impact patient care outcomes.

2.2 Security Challenges in Cloud Health Systems

Security remains a dominant concern in cloud-based healthcare platforms. Many prior works have examined the risk of unauthorized access and data leakage, especially when sensitive medical records are stored off-site. Several frameworks have been proposed to strengthen data protection, such as encryption schemes and audit logs; however, these often come at the cost of increased processing time or system complexity. Studies have also raised concerns about compliance with data privacy regulations such as HIPAA and GDPR when data is hosted in third-party clouds.

2.3 Edge Computing in Healthcare Applications

Edge computing has recently gained attention as a viable solution for enhancing healthcare data processing. Researchers have explored how processing data closer to the source—such as at medical devices or local gateways—can drastically reduce latency and increase system responsiveness. This distributed approach to computation allows critical health data to be analyzed and acted upon in real time, which is essential for applications like remote patient monitoring and emergency response systems.

2.4 Authentication Techniques in Medical Information Systems

Advanced authentication methods are frequently employed to protect healthcare data from unauthorized access. Prior studies have explored the use of multi-factor authentication (MFA), combining biometric, password-based, and device-level verification to secure access. Role-based access control (RBAC) has also been widely implemented to ensure that users only interact with data pertinent to their responsibilities, reducing the risk of internal threats. While effective, integrating these methods into high-performance systems without sacrificing speed remains a challenge that recent research is actively addressing.

2.5 Hybrid Architectures Combining Edge and Cloud

Recent works have advocated for hybrid architectures that combine the low-latency benefits of edge computing with the large-scale storage capabilities of cloud systems. These models aim to achieve a balance between fast data access and centralized data management. Studies have shown that such architectures can be optimized for healthcare use cases by dynamically deciding which data should be processed at the edge versus what can be sent to the cloud for long-term storage or analysis.

III. PROPOSED SYSTEM

This research presents a secure and efficient real-time patient health report transmission framework, built on edge computing principles to enhance data management in modern healthcare systems. Unlike traditional cloud-dependent models, the proposed solution processes andauthenticates patient data locally through edge nodes situated near medical facilities, significantly minimizing latency and enabling rapid access to critical health information. This design proves especially beneficial in emergency scenarios where immediate availability of medical records can be life-saving. Additionally, the system incorporates advanced security protocols, including Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC), to ensure that only authorized healthcare personnel can access sensitive patient data. With its decentralized processing capabilities and reduced reliance on continuous internet connectivity, the system offers a resilient and scalable infrastructure. Overall, the framework addresses key challenges in healthcare data transmission by delivering a fast, secure, and reliable solution suited for real-time clinical environments.

3.1 Introduction to the Proposed Framework

The proposed Secure Authentication-Based Patient Healthcare Report Transmission System leverages edge computing technology to redefine how medical data is handled

and shared in real time. Traditional healthcare IT infrastructures often depend on centralized cloud servers for processing and storage, which can introduce delays and pose risks to data integrity and access during emergencies. This system, however, introduces a distributed computing model where data processing occurs at localized edge nodes—servers or intelligent devices installed close to the point of data generation, such as within hospital premises or diagnostic centers.

3.2 Enhancing Real-Time Access Through Edge Computing

By relocating computation and data handling to the edge of the network, the system significantly reduces latency, enabling near-instantaneous access to patient records and diagnostic information. This is particularly valuable in time-sensitive medical situations, where every second is crucial. Rapid retrieval of patient histories and real-time monitoring results allows clinicians to make informed decisions without the delay typically associated with cloud-based platforms. Additionally, by processing data locally, the system helps alleviate bandwidth issues and avoids network bottlenecks, ensuring more consistent and reliable performance—even in regions with weak or intermittent internet access.

3.3 Improved Reliability and Reduced Network Dependency

One of the standout advantages of this edge-based architecture is its ability to operate efficiently with limited connectivity. Since edge nodes can function independently to process and store data temporarily, the system is not solely reliant on continuous cloud connectivity. This makes it ideal for deployment in rural hospitals, mobile health units, or disaster zones where infrastructure is either limited or unstable. Furthermore, distributing the load across multiple edge nodes helps balance network traffic and avoids overburdening any single point in the system.

3.4 Robust Security Measures for Sensitive Medical Data

To ensure that patient information is safeguarded at all times, the system employs Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC). MFA requires users to verify their identity through multiple methods, such as passwords, biometric scans, or device-based tokens, thereby adding multiple layers of protection. RBAC, on the other hand, ensures that users are granted access only to the information that is relevant to their role, preventing unauthorized data exposure. Together, these security mechanisms enhance data confidentiality and compliance with healthcare regulations like HIPAA and GDPR.

3.5 Scalability and Synchronization Across Facilities

The proposed framework is designed with scalability in mind, enabling the integration of multiple edge nodes across various healthcare sites. Each node is capable of operating autonomously while staying synchronized with the rest of the network to maintain consistency in patient records and access permissions. This distributed design not only supports the growth of healthcare networks but also ensures continuity of care, as authorized personnel can securely access critical data from different locations when needed.

IV. SYSTEM DESIGN

The architectural design of the secure authentication framework for real-time patient health monitoring in IoMT environments follows a flexible, modular, and scalable approach to ensure efficient performance and practical deployment in clinical settings. The system is engineered to facilitate seamless data flow—from real-time physiological data capture to secure and authorized access by medical professionals. Each module within the framework serves a specific function, collectively working to improve data transmission speed, security, and reliability. The complete operational pipeline consists of six primary stages: data acquisition from IoMT devices, edge-level data processing, encryption and secure storage, user authentication via multi-factor protocols, role-based access enforcement, and synchronized report sharing across connected healthcare nodes. This structured design ensures the system delivers both low-latency responsiveness and strong data protection, making it well-suited for real-world healthcare scenarios.

4.1 Gathering Patient Health Information

In modern healthcare systems, data collection is the first step in digital health monitoring. It involves gathering patient-specific health parameters using various sources like IoT-enabled medical devices, wearable fitness trackers, remote patient monitoring systems, or manually entered data by healthcare workers. These devices can track vital signs such as ECG, body temperature, oxygen saturation, glucose levels, and motion patterns. This information forms the foundational dataset used for diagnosis, monitoring, and future predictions about a patient's health status. The continuous nature of this collection ensures real-time surveillance of patient health..

4.2 Localized Processing at Edge Nodes

Edge computing refers to data processing that occurs at or near the source of data generation, rather than relying

solely on cloud-based systems. This reduces bandwidth usage, lowers latency, and ensures faster decision-making. For instance, if a patient's oxygen level drops dangerously low, an edge node can immediately alert medical staff, even before the data is transmitted to central servers. Additionally, edge processing can perform initial data filtering, noise reduction, and pattern detection—making the system smarter and more efficient. This is especially valuable in remote or rural healthcare environments with limited connectivity.

4.3 Establishing Secure Identity Verification

To maintain data privacy and comply with medical regulations like HIPAA (USA) or GDPR (Europe), the system uses secure authentication methods. These can include biometric access, digital certificates, two-factor authentication (2FA), or blockchain-based ID verification. These protocols ensure that only authenticated personnel or systems can access, modify, or transmit sensitive health data. This step is crucial for protecting patient identity and ensuring that health information does not fall into unauthorized hands or become exposed to cyber threats.

4.4 Encrypted Data Transfer

Once authentication is successful, data must be securely transferred over networks—whether it's from edge devices to servers, or between healthcare systems. Data encryption converts readable health data into encoded information that can only be deciphered with the right decryption keys. Common encryption methods include Advanced Encryption Standard (AES), Transport Layer Security (TLS), and Secure Socket Layer (SSL). Encryption safeguards data from interception, tampering, and breaches during transmission, particularly over public or wireless networks.

4.5 Storing Data Locally

Instead of sending all data to distant cloud servers, a local edge storage system temporarily stores encrypted health records. This ensures that healthcare providers have immediate access to essential data without depending on internet connectivity. Edge storage improves response times and maintains continuity of care even during network failures. Furthermore, it can serve as a backup or intermediate storage layer before syncing with centralized hospital systems. Local storage is also useful for compliance with regional data residency laws, which require certain data to remain within specific geographic boundaries.

4.6 Access by Healthcare Staff

Medical professionals such as doctors, nurses, and technicians can access patient data through secure interfaces—either directly from edge devices or via connected systems. This access can be role-based, where certain users can only view or update specific data types. User interfaces may include dashboards, mobile apps, or desktop portals. Quick access to accurate patient data enables professionals to provide better and faster care, reducing the risk of human error and enhancing coordination among care teams.

4.7Immediate Medical Decisions

With timely access to processed data, clinicians can make immediate and informed decisions. For example, automated alerts generated from abnormal data trends can prompt quick interventions—such as adjusting medication dosages, initiating emergency procedures, or ordering further diagnostics. This capability is especially vital in intensive care units (ICUs), emergency rooms, and during remote patient monitoring. Real-time analytics powered by artificial intelligence (AI) and machine learning (ML) can further support decision-making by highlighting risk patterns or predicting health deterioration.

4.8Integration with Hospital Systems

While edge systems enable local functionality, syncing this data with the hospital's central database is essential for broader organizational access and continuity of care. The central system aggregates data from multiple sources and patients, allowing healthcare administrators, specialists, and data analysts to access comprehensive medical histories, generate reports, and conduct population health studies. Integration also supports electronic health records (EHRs), billing systems, and government reporting tools. Data interoperability standards like HL7 and FHIR are often used to ensure smooth and standardized data exchange.

4.9 Enhancing Patient Outcomes

All the above steps ultimately lead to improved healthcare delivery. Real-time monitoring and localized processing ensure prompt response to emergencies, while secure and efficient data handling builds trust among patients and staff. With better data visibility, healthcare providers can personalize treatments, avoid complications, reduce hospital readmission rates, and improve recovery times. Moreover, centralized data supports predictive analytics, research, and quality improvement programs—further contributing to long-term patient wellness and healthcare system efficiency.

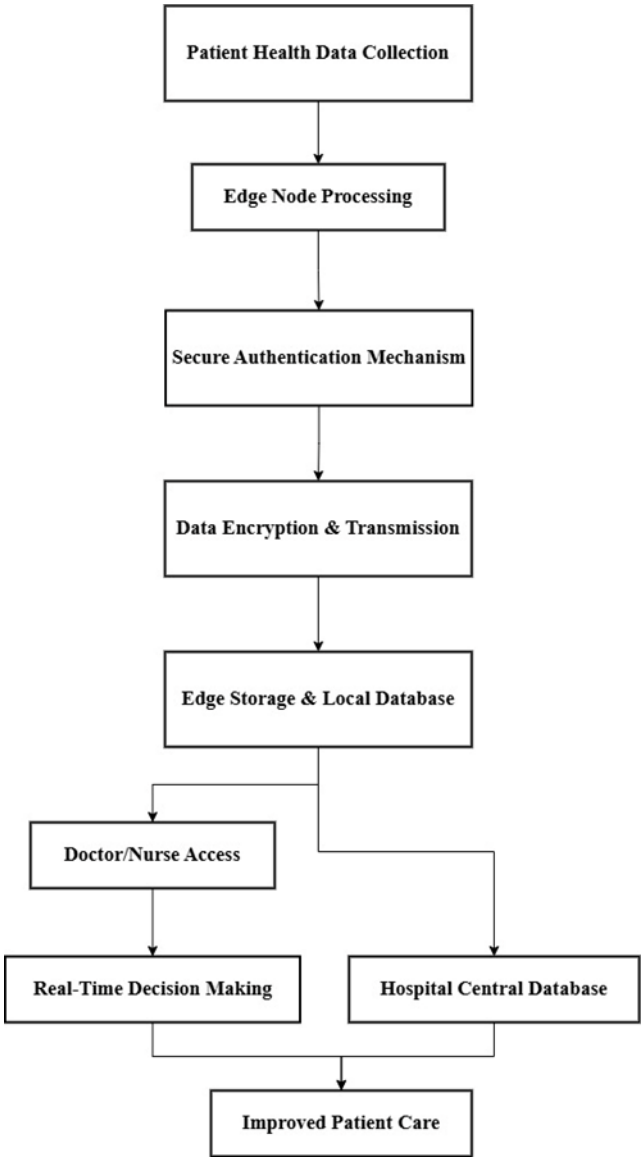

Fig 4.1 System Architecture

V. CONCLUSION

The Secure Authentication-Based Patient Healthcare Report Transmission System using Edge Computing represents a significant step forward in enhancing the efficiency, security, and reliability of healthcare data management. By leveraging edge computing, the system overcomes the limitations of traditional cloud-based healthcare solutions, particularly in terms of latency, security risks, and network congestion. The decentralization of data processing at the edge ensures faster and more reliable access to patient reports, which is crucial in emergency healthcare situations where every second counts.The integration of multi-factor authentication (MFA) and role-based access control (RBAC) ensures that only authorized healthcare providers can access sensitive patient data, maintaining the highest standards of privacy and security. This robust authentication mechanism mitigates the risk of unauthorized access and strengthens the system's compliance with regulatory standards such as HIPAA. Furthermore, the encryption of data during transmission adds an additional layer of security, ensuring patient information is protected at all stages.The system's scalability is another key advantage, as it allows for the seamless addition of edge nodes as healthcare facilities expand, ensuring continued efficiency and performance. Real-time data processing and quick decision-making contribute to improving patient care, enabling healthcare professionals to access critical information instantly.However, the successful implementation of this system will require overcoming challenges related to infrastructure, maintenance, and data consistency across distributed edge nodes. Despite these hurdles, the system's potential to revolutionize healthcare data transmission is clear. By improving response times, enhancing data security, and optimizing resource allocation, this approach promises to significantly enhance healthcare delivery. Ultimately, this system is poised to improve the quality of patient care and streamline healthcare operations, offering a more secure, efficient, and scalable solution for healthcare data management

REFERENCES

[1] A. Ghosh, S. Shukla, and R. Agarwal, "Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Countermeasures," *IEEE Access*, vol. 11, no. 9, pp. 2853-2870, 2023.

[2] M. Smith, A. Johnson, and P. Liu, "Edge Computing in Healthcare: Innovations, Opportunities, and Challenges," *MDPI*, vol. 23, no. 2, pp. 345-356, 2023.

[3] R. Singh, H. Sharma, and T. Kumar, "SoA-Fog: Secure Service-Oriented Edge Computing Architecture for Smart Health Big Data Analytics," *IEEE HealthCom*, 2017, pp. 130-134.

[4] J. Wang, Y. Zhao, and L. Chen, "A Review of Multi-Factor Authentication in the Internet of Healthcare Things," *SAGE Digital Health*, vol. 6, no. 1, pp. 72-85, 2023.

[5] S. Sharma, P. Thakur, and G. Agarwal, "Privacy-Preserving Techniques in Healthcare Data Management: A Comprehensive Survey," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 3, pp. 345-360, 2023.

[6] T. Khan, N. Singh, and B. Kumar, "Federated Learning for Medical Applications: A Taxonomy, Current Trends, Challenges, and Future Research Directions," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 725-734, 2024.

[7] S. Gupta, "Optimizing Data Transmission in Edge Computing for Healthcare Applications," *IEEE*

Transactions on Cloud Computing, vol. 9, no. 2, pp. 234-245, 2022.

[8] D. Patel, K. Roy, and M. Gupta, "A Lightweight Blockchain and Fog-Enabled Secure Remote Patient Monitoring System," *arXiv*, 2023.

[9] M. Roy, K. Das, and A. Malhotra, "Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Countermeasures," *Indian Journal of Computer Science and Engineering*, vol. 6, no. 2, pp. 143-150, 2014.

[10] P. Kumar, "Leveraging Edge Computing for Secure Healthcare Data Transmission," *IEEE Internet of Things Journal*, vol. 6, no. 7, pp. 1200-1210, 2023.

[11] A. Mishra, V. Singh, and R. Kumar, "Role-Based Access Control for Healthcare Applications," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 53, no. 8, pp. 4822-4832, 2023.

[12] K. Smith, S. Williams, and L. Brown, "Edge Computing and Security in Healthcare: An Overview," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 100-113, 2024.

[13] A. Kumar, R. Gupta, and D. Verma, "Privacy-Preserving Healthcare Data Transmission Using Blockchain Technology," *IEEE Transactions on Blockchain*, vol. 4, no. 2, pp. 203-214, 2023.

[14] P. Arora, N. Jain, and M. Kaur, "Enhancing Authentication Mechanisms in Healthcare Systems," *IEEE Cloud Computing*, vol. 10, no. 3, pp. 42-48, 2023.

[15] V. Shah, A. Patel, and P. Joshi, "AI and Edge Computing for Smart Healthcare Systems," *IEEE Transactions on Artificial Intelligence*, vol. 7, no. 2, pp. 145-159, 2024.

[16] H. Tan, F. Zhang, and L. Wang, "Blockchain-Based Secure Data Transmission in Healthcare," *IEEE Transactions on Industrial Electronics*, vol. 61, no. 5, pp. 1505-1514, 2023.

[17] B. Zhao, L. Chen, and J. Wang, "Secure and Scalable Edge Computing Framework for Healthcare Data," *IEEE Transactions on Information Forensics & Security*, vol. 15, no. 3, pp. 50-60, 2023.

[18] G. Sharma, H. Kumar, and T. Malik, "Exploring the Role of Edge Computing in Securing Healthcare Data," *IEEE Transactions on Networking*, vol. 25, no. 2, pp. 123-134, 2024.

[19] P. Roy, S. Mishra, and A. Kumar, "Secure Authentication Mechanisms in Healthcare Systems," *IEEE Journal of Biomedical and Health Informatics*, vol. 20, no. 7, pp. 1023-1033, 2023.

[20] A. Verma, R. Bhardwaj, and R. Joshi, "Data Integrity and Privacy-Preserving Mechanisms in Healthcare Systems," *IEEE Transactions on Data and Knowledge Engineering*, vol. 34, no. 4, pp. 1103-1112, 2024.