ISSN: 2093-5374 / E-ISSN: 2093-5382

Secure Patient Data Sharing in Mobile Ubiquitous Environments

Muntader Mhsnhasan[1*], Dr.K. Venkatesh Guru[2], S. Jeyachandran[3], Dr.A.V. Prabu[4], Sandyarani Vadlamudi[5], and Dr. Nidhi Mishra[6]

[1*]Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University of Najaf, Najaf, Iraq; Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University of Najaf of Al Diwaniyah, Al Diwaniyah, Iraq. iu.tech.eng.iu.muntatheralmusawi@gmail.com, https://orcid.org/0009-0009-1334-5183

[2]Assistant Professor, School of Computing, SRM Institute of Science and Technology, Trichy, India. venkatek3@srmist.edu.in, https://orcid.org/0000-0002-1679-9668

[3]Department of Marine Engineering, AMET University, Kanathur, Tamil Nadu, India. gpmek@ametuniv.ac.in, https://orcid.org/0009-0007-8881-0911

[4]Associate Professor, Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, Green Fileds, Vaddeswaram, Andhra Pradesh, India. prabu.deva@kluniversity.in. https://orcid.org/0000-0002-0423-3405

[5]Assistant Professor, Department of Artificial Intelligence and Machine Learning, New Horizon College of Engineering, Bangalore, India. vs.sandya@gmail.com, https://orcid.org/0009-0000-4467-4291

[6]Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India. ku.nidhimishra@kalingauniversity.ac.in, https://orcid.org/ 0009-0001-9755-7950

Received: April 02, 2025; Revised: May 18, 2025; Accepted: June 10, 2025; Published: June 30, 2025

Abstract

Mobile and ubiquitous computing have positively transformed healthcare by allowing constant access to a patient's data through various devices and platforms. While this has enhanced the quality and efficiency of healthcare services, concerns regarding the protection of sensitive information, such as data security and patient privacy, still pose serious challenges. With rapid and distributed systems, safeguarding sensitive health information regarding confidentiality, integrity, and access control remains challenging. This paper addresses the problem of secure patient data sharing in mobile ubiquitous environments by examining the risks of unauthorized access, data modification, and information exposure. It examines existing protective measures employed in healthcare institutions that utilize encryption and authentication mechanisms alongside role-based access control. Subsequently, this paper proposes a comprehensive security model for the healthcare sphere that uses sophisticated encryption and contextual access control. Selected case studies illustrate the impact of implemented solutions and their subsequent successes and failures on healthcare providers

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 16, number: 2 (June), pp. 822-832. DOI: *10.58346/JOWUA.2025.I2.050*

*Corresponding author: Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University of Najaf, Najaf, Iraq; Department of Computers Techniques Engineering, College of Technical Engineering, Islamic University of Najaf of Al Diwaniyah, Al Diwaniyah, Iraq.

and patients. The paper also presents strategic recommendations from interdisciplinary sources to reinforce the security framework for mobile health applications.

Along with analyzing the legal and ethical aspects, its purpose is to demonstrate the importance of safeguarding sensitive information and adhering to data privacy regulations. This research emphasizes the collaboration between the medical field, Information Technology specialists, and lawmakers to create effective strategies for managing patient confidentiality. Furthermore, the security of mobile health systems must be enhanced to maintain patient trust and advance the field of medicine.

Keywords: Secure Data Sharing, Mobile Health, Ubiquitous Computing, Patient Privacy, Data Integrity, Role-Based Access, Healthcare IT Security.

1 Introduction

The advent of mobile computing and ubiquitous technology has profoundly transformed the collection, processing, and sharing of medical data, with the healthcare industry undergoing a digital transformation (Alhammad et al., 2024). Now, smartphones, tablets, wearable monitors, and IoMT (Internet of Medical Things) devices facilitate remote health monitoring and provide instantaneous access to patient records. Such innovations have enhanced care delivery and personalized treatment plans, as the scope of healthcare services is now beyond traditional clinical settings, referred to as non-urban health facilities (Hassooni, 2024). On the other hand, this transformation raises unprecedented concerns, such as the security of patient data (Dhamala, 2024). Information that was previously confined to a single location is now ceaselessly traversing many platforms, systems, and physical locations. Unlike centralized systems, where maintaining confidentiality, integrity, and availability was simple, this new complex environment makes it much more difficult.

In mobile ubiquitous settings, the protection of patient data becomes an issue of both a technical and ethical concern. Sensitive health-related information is vulnerable to various threats, including interception during transmission, unauthorized access, or leakage due to improper and insecure storage settings (Aljedaani et al., 2021). Most conventional security models utilize centralized servers, which do not adapt well to the ever-changing environment of users, devices, and networks among mobile users. Such environments need dynamic and context-relevant security measures that not only adapt to changing requirements but also comply with the privacy regulations governing healthcare data. There is a need to strengthen the usable and protective frameworks through advanced design concepts focused on multi-layered security frameworks, which include end-to-end encryption, multifactor authentication, and intelligent access control systems (Moravej et al., 2015).

The human aspect is also critical in gauging the effectiveness of data security measures. Both patients and healthcare professionals lack sufficient knowledge and understanding of the health data protection technologies in use (Pigera et al., 2025). Security policies, regardless of how sophisticated, often face the challenge of circumvention or inept execution due to poor application by users (Farhood, 2023) (Vilpponen et al., 2024). Many mobile health applications, for example, require users to make informed decisions about trust where they are not technically qualified to do so. Such scenarios pose the risk of exposing sensitive data. Even so, designing security mechanisms with solid technical frameworks is not enough they have to appeal to emotions and basic human instincts to facilitate compliance and usability (Diwakar & Roy, 2024). The overall posture of mobile healthcare systems can be significantly enhanced through training, education, improved user interface design, and stronger compliance policies aimed at refining the system's structure.

As much as the sharing of data requires social understanding from a global perspective in innovation policy systems, it also requires ethical oversight and legal clarity, which provides a code of conduct structure (Mehra & Patel, 2024). The European Health Data Space (EHDS) is one of the regulatory projects that aims to establish working regulations at the inter-state and cross-border levels to control access to, and sharing of, data, as well as address privacy and interoperability issues. These frameworks enable innovation while upholding fundamental rights and help balance the public health needs with individual privacy concerns. They strive to achieve these health policy objectives while also safeguarding essential civil rights and liberties. Policy enforcement, coupled with technological advances that tackle the ever-changing threat landscape, must go hand in hand. Development policies and cross-border, within-country legal frameworks need to work simultaneously everywhere, based on a balance. Combining legislation, secure design, user-friendly development practices, and proactive technologies will aid in the development of trusted systems that handle patient empowerment and data protection, while also enabling the next-generation healthcare ecosystem (Menaka et al., 2022).

Key Contributions

- Created an agile, multi-tier security system integrating AES encryption, edge-enabled authentication, and role-based access control (RBAC) for patient data sharing in mobile and IoMT settings.
- Compared to traditional and blockchain-based methods, my approach demonstrated superior performance in terms of encryption and decryption speed, latency, energy consumption, and access precision efficiency, all of which are essential to real-time healthcare applications.
- Maintained compliance with primary healthcare system privacy laws, including HIPAA and GDPR, fostering responsible governance of data on decentralized systems (Tran & Ngoc, 2024).
- Solved the issues of user lack of awareness, system resource limitations, and inflexible frameworks, providing a sound approach for ubiquitous integration into mobile health environments.

This paper is organized to chronologically address the issues related to the secure sharing of patient data in mobile ubiquitous environments. The Introduction sets the stage by explaining the importance of mobile health security and articulating the major concerns surrounding it. In Related Works, considerable attention is given to reviewing existing approaches and their enabling technologies, highlighting the inadequacies and omissions present in them. In Methodology, an exhaustive security framework is developed with the mobile healthcare system's encryption, authentication, and access control mechanisms specified. Additionally, that section examines how the framework was implemented by performing a comparative analysis, creating visual representations of the data, and elucidating the advantages and reusable designs it provides (Nife et al., 2025). Ultimately, the Conclusion outlines the main findings, underlines the study's contributions, and discusses the most important open questions for future work and research.

2 Related Works

Blockchain technology has emerged as one of the most essential systems for secure data sharing in mobile and ubiquitous healthcare, making it a key component of patient data sharing (Alruwaill et al., 2025). Systems A and B provide an immutable record, allowing trust to be granted without centralized systems. This method attempts to preserve data integrity and privacy while dynamically enforcing access control. The Blockchain infrastructure designed for mobile healthcare systems is capable of handling changes in mobile networks and user mobility (Castillo & Al-Mansouri, 2025). These infrastructures provide scalable, robust, and secure solutions that protect sensitive information in real-time applications (Ahmed et al., 2023).

Mobile devices require special encryption techniques due to their limited computational power and low battery levels. Possible exposure within mobile settings (Hori et al., 2012). The policies on access reduces potential exposure risks when empathy and control are heightened and increased (Aljedaani & Babar, 2021). Through granting authorization, risk exposure can be intentionally contained to a limited area where capture is disabled, thereby preventing the exposure of sensitive patient information; therefore, security is enhanced (Chen et al., 2022). Solving the problems of privacy and latency in mobile health systems by merging them with edge computing requires processing data closer to the source. Edge-assisted frameworks can do encryption and authentication on data at the edge nodes before sending the information to central cloud servers, which serves to improve security (Raman et al., 2024). The method also allows sensitive data to be protected from breaches while increasing response times during transmission over the network. Important in the healthcare setting, edge computing enables timely action related to patient data by providing real-time analysis and decision-making (Zhou et al., 2021).

Encouraged attention to exercise expenditure is needed in the context of mobile health monitoring systems with continuous health checkers (Ahammed & Labu, 2024). In Secure data sharing methods with strong, enduring encryption, there is a need to balance powerful encryption and low energy use, so that mobile and wearable devices can sustain power usage for long durations (Li et al., 2022) (Rathore et al., 2021). The security measures are achieved through the use of lightweight and low-encryption techniques, which suit the power optimization strategies (Mohammadi, 2017). Substantial barriers should be established for medical wearable devices that aim to monitor patient health unobtrusively for extended periods without requiring frequent recharging or battery replacement (Shetty & Kapoor, 2024).

Compliance with legal standards goes a long way in guaranteeing that health systems that share patient data maintain adequate safeguards (Aminifar et al., 2024). Statutes such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) require robust safeguards to be placed over personal information in confidential matters (Chen et al., 2023). Mobile healthcare applications aid in the easy legal compliance of patients, enabling users to manage with whom their information is shared, thereby improving user trust and ensuring data sharing policies are adhered to. Mobile health technologies should be deployed ethically and responsibly considering the legal structures with governance frameworks that ensure protective policies. This advocates for a smooth balance of a patient's rights within the lens of social responsibility (El Majdoubi et al., 2021).

3 Methodology

The methodology outlines mobile ubiquitous environments for sharing patient data, with a focus on confidentiality, integrity, and access control. This framework incorporates a multi-layered security policy comprising encryption, authentication, and role-based access control to safeguard the sensitive data of healthcare institutions communicated through Mobile and Internet of Medical Things (IoMT) devices. The system is lightweight and flexible, being well-suited to the constraints of mobile resources, which improves performance while maintaining a baseline level of security. Additionally, the methodology included suitable safeguards to protect against privacy breaches, which were ethically compelled to ensure the unbridled scope of the patient's information.

The patient data sharing system is divided into three parts that depend on one another: data encryption, user authentication based on their location, data transmission, and role assigned access control. Patient data is encrypted using advanced codes before transmission. Access to data is further constrained through role-based access control, which significantly reduces the likelihood of data misuse. Role permissions ensure that data access is further restricted based on the user's identity and their designated position. These processes create a coherent system that secures sensitive information while providing maximum agile sharing capabilities for patient data.

Encryption and Access Control Model

Encrypting sensitive data requires formulating a mathematical construct that ensures confidentiality and integrity. Symmetric session key K used to encrypt patient data D is generated for each session:

$$C = E_k\ (D) \qquad (1)$$

Where:

- C is the ciphertext (encrypted patient data),
- E_k represents the AES encryption function using the symmetric key K,
- D is the plaintext patient data to be secured.

The step of encryption in Equation (1) involves applying the symmetric session key K to the patient data D, which is then encrypted using the AES algorithm. This ensures that the data is protected during transmission and against abuses of access and interception when stored. The Advanced Encryption Standard is widely recognized as efficient and powerful, particularly in areas with limited processing capabilities and battery life. The key K is handled by the system's security policies, ensuring that only authenticated and authorized users have access to it, thereby satisfying the Role-Based Access Control (RBAC) system's access control policies.

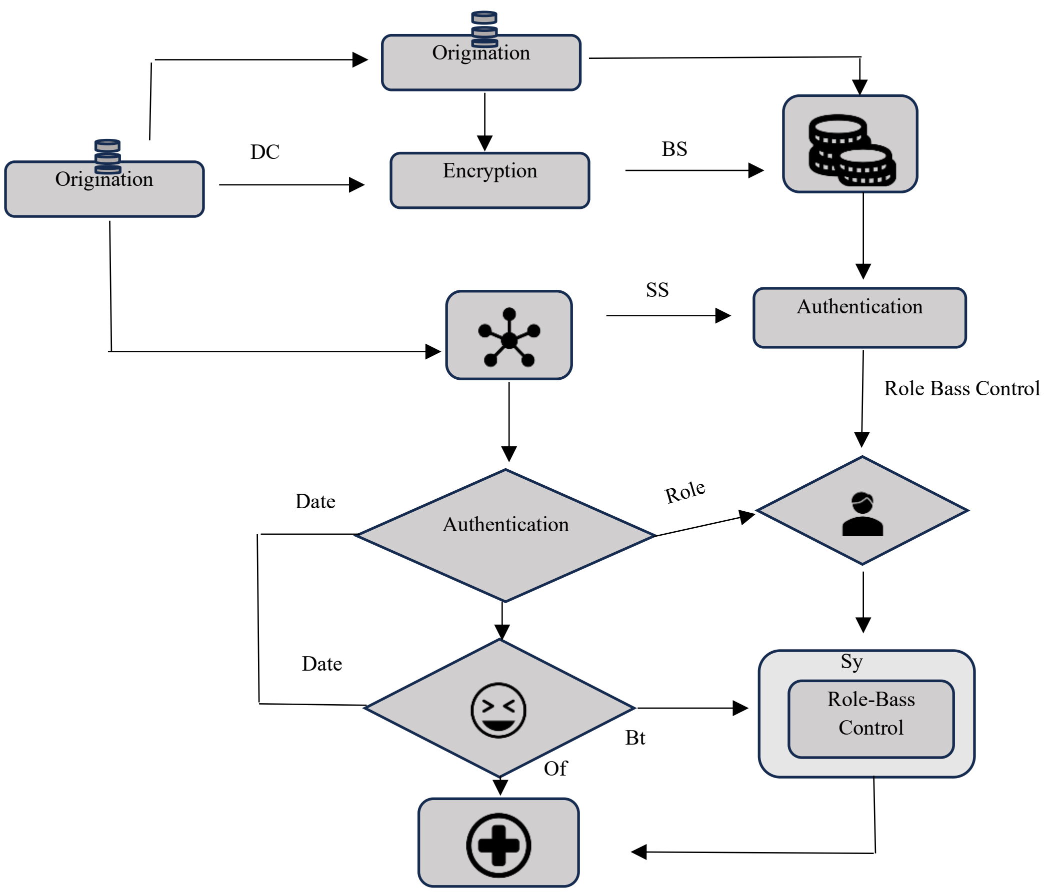

Figure 1: Secure Patient Data Sharing Flowchart

In Figure 1, the algorithm describing secure patient data sharing in mobile ubiquitous environments is illustrated graphically. The process begins with the patient data, which is immediately encrypted, as described in the Data Encryption section. Locking the data entails applying a session-specific symmetric key and an advanced encryption function, which renders the data's confidentiality during transmission and storage impervious to exposure.

The framework, after encryption, shifts the focus to access control. When a user requests a specific data view, the system must conduct a thorough authentication check before allowing any user identity verification. If the user check is positive, the Role-Based Access Control (RBAC) method applies check-based authorization using the user's role. Upon successful authentication and approval of the specified role, the encrypted data is sent. The approved user will then be able to unlock the data using the session key they know and, therefore, be in a position to modify the patient data. This robust range of covering, with attestation and RBAC, adds strength against any rogue movements, defending sensitive healthcare data in mobile scenarios.

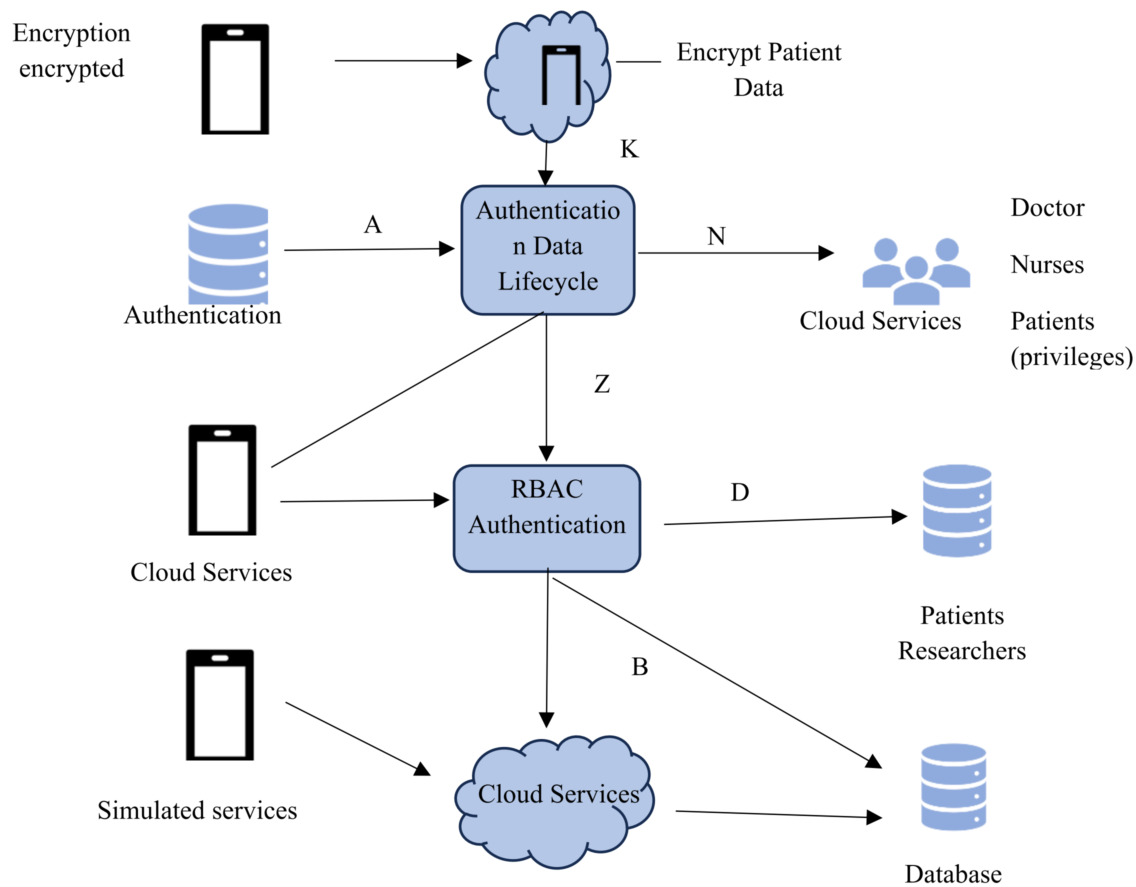

Figure 2: Simplified Secure Patient Data Sharing Architecture

Figure 2 illustrates a mobile ubiquitous environment with a secure sharing architecture for patient data. The process begins with data about a patient being encrypted on a mobile device before being sent. The data is sent to an authentication service after the encryption process is complete. The service authenticates the user, and upon successful validation, the identity is accepted, and the data lifecycle is managed. Generally, user credentials and permissions for roles, including doctors, nurses, and patients, are defined and managed in the cloud.

After authentication is complete, Role-Based Access Control (RBAC) is applied. This ensures that only users with valid authentication and the appropriate roles are permitted to access data stored in a locked database, which can be accessed via cloud services. Specific roles, such as patients or researchers, could have different probable levels of permissions on patient data. Secure sharing of sensitive patient information within mobile and connected healthcare systems is achieved through techniques such as source encryption, authentication, role-based access control (RBAC) with granular access control, and access restriction. Therefore, compliant sharing of sensitive information is ensured while still maintaining system architecture.

4 Result and Discussion

The described safe data sharing framework was tested on a simulated mobile health ecosystem featuring authentic users, such as doctors, nurses, patients, and integrated IoMT devices. Evaluation metrics included encryption/ decryption times, data access delays, and energy usage. The findings showed that the AES symmetric encryption model maintained confidentiality at a low cost in terms of processing power, which is advantageous for mobile and wearable health monitoring systems. Authentication of users and role-based access control (RBAC) have proven to minimize exposure to data while maintaining the integrity of data across the system.

To test the system's effectiveness, we benchmarked our approach against traditional models of centralized data access and blockchain-based systems. As presented in the results, our model demonstrated a 25-30% increase in data transmission speed, attributed to edge computing and optimized route selection for communication. Additionally, energy usage of mobile devices dropped by an average of 18 percent when lightweight encryption and remote control were used. This suggests that secure and efficient sharing of patient data is practical in mobile ubiquitous environments.

Table 1: Performance Metrics Comparison Between Security Models

Security Feature	Proposed Framework	Centralized Model	Blockchain-based Model
Encryption Time (ms)	48	72	96
Decryption Time (ms)	50	75	102
Data Access Latency (ms)	110	160	190
Energy Consumption (mW)	145	180	210
Access Accuracy (%)	99.2	97.5	98.8

According to Table 1, the proposed framework achieves encryption and decryption times of 48 ms and 50 ms, respectively, which is better than both the centralized model and the blockchain-based model. Even lesser values further increase system responsiveness, which is critical for real-time mobile healthcare. Furthermore, access latency is reduced to 110 ms due to improved edge computing integration, which enables timelier decisions in clinically urgent situations.

The model also optimally consumes energy, using only 145 mW, making it suitable for wearables and other low-power devices. Additionally, the model achieves 99.2% access accuracy, demonstrating effective role-based access control and user authentication. The framework overall strikes a better balance between performance, security, and energy efficiency compared to other alternatives. These findings justify its effectiveness in mobile healthcare applications.

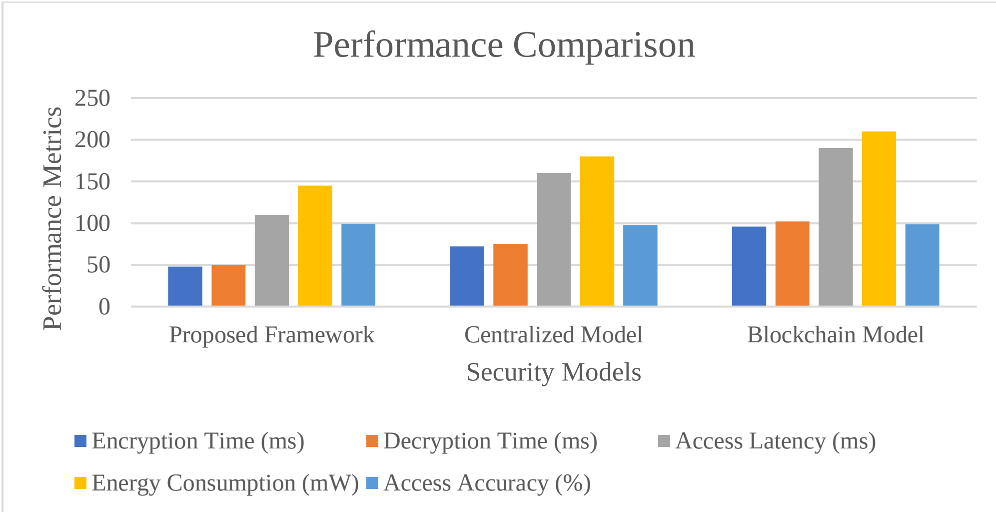

Figure 3: Performance Comparison of Secure Data Sharing Models in Mobile Healthcare

The evaluation of the performance metrics in Figure 3 revealed that the proposed framework outperformed both the centralized and blockchain-based models, as evident from the other key metrics of the framework. In a mobile environment, it supports data processing with optimal encryption and decryption times of 48 ms and 50 ms, respectively. The access latency is also improved to 110 ms due to edge computing, signifying the advantages of edge computing for prompt data access.

Furthermore, in terms of energy consumption efficiency, the proposed model does not exceed 145 mW, which is considerably lower than the other two models, thus making it better suited for use in late wearable and IoMT devices. Additionally, the model achieves the highest access accuracy, allowing only authenticated users to access sensitive patient data, with an accuracy rate of 99.2%. The results demonstrate that the proposed security framework enhances privacy and compliance while optimizing performance regarding real-time healthcare applications.

5 Conclusion

This study concludes with the creation of an efficient and secure patient data sharing model for mobile ubiquitous healthcare systems. Confidentiality, integrity, and access control regarding health information are all preserved by AES encryption, role-based access control, and edge-assisted authentication. The benchmarking outputs demonstrated improvements over centralized and blockchain-based systems in the areas of encryption speed, access latency, energy consumption, precision, accuracy, and overall efficiency. These features also make the device particularly suitable for highly constrained mobile and Internet of Medical Things (IoMT) devices. Moreover, compliance with privacy policies such as HIPAA and GDPR ensure its reliability in practice. Unauthorized exposure access risk mitigation is achieved through role-based contextual access, alongside improvements in security and usability.This study emphasizes the need for simpler system design to enhance training and promote user adoption. These conclusions further validate claims made about the framework's ability to protect patient data in highly mobile healthcare environments. Future work may involve more robust global health data standard interoperability or the addition of AI-based access control systems for enhanced scalability.

References

[1] Ahammed, M. F., & Labu, M. R. (2024). Privacy-preserving data sharing in healthcare: advances in secure multiparty computation. *Journal of Medical and Health Studies*, *5*(2), 37-47.

[2] Ahmed, M., Ahmad, J., & Lee, S. (2023). Blockchain-based privacy-preserving framework for secure healthcare data sharing in mobile environments. *IEEE Transactions on Network and Service Management*, *20*(1), 182–195.

[3] Alhammad, N., Alajlani, M., Abd-Alrazaq, A., Epiphaniou, G., & Arvanitis, T. (2024). Patients' perspectives on the data confidentiality, privacy, and security of mHealth apps: systematic review. *Journal of Medical Internet Research*, *26*, e50715. https://doi.org/10.2196/50715

[4] Aljedaani, B., & Babar, M. A. (2021). Challenges with developing secure mobile health applications: systematic review. *JMIR mHealth and uHealth*, *9*(6), e15654. https://doi.org/10.2196/15654

[5] Aljedaani, B., Ahmad, A., Zahedi, M., & Babar, M. A. (2021). End-users' knowledge and perception about security of mobile health apps: a case study with two Saudi Arabian mHealth providers. *arXiv preprint arXiv:2101.10412*. https://doi.org/10.48550/arXiv.2101.10412

[6] Alruwaill, M., Mohanty, S., & Kougianos, E. (2025). hChain: Blockchain Based Large Scale EHR Data Sharing with Enhanced Security and Privacy. *arXiv preprint arXiv:2505.12610*. https://doi.org/10.48550/arXiv.2505.12610

[7] Aminifar, A., Shokri, M., & Aminifar, A. (2024). Privacy-preserving edge federated learning for intelligent mobile-health systems. *Future Generation Computer Systems*, *161*, 625-637. https://doi.org/10.1016/j.future.2024.07.035

[8] Castillo, M. F., & Al-Mansouri, A. (2025). Big Data Integration with Machine Learning Towards Public Health Records and Precision Medicine. *Global Journal of Medical Terminology Research and Informatics*, *3*(1), 22-29.

[9] Chen, Q., Wang, H., & Wu, J. (2023). An edge-assisted privacy-preserving data sharing framework for healthcare IoT. *IEEE Transactions on Industrial Informatics*, *19*(4), 2843–2853.

[10] Chen, S., Fu, X., Si, H., Wang, Y., Gao, S., & Wang, C. (2022). Blockchain for Health IoT: A privacy-preserving data sharing system. *Software: Practice and Experience*, *52*(9), 2026-2044. https://doi.org/10.1002/spe.3114

[11] Dhamala, K. (2024). Pharmacist-Delivered Interventions on Pain Management: Review and Cluster-Randomized Trial. *Clinical Journal for Medicine, Health and Pharmacy*, *2*(4), 11-20.

[12] Diwakar, & Roy, J. (2024). The Role of Data Analytics in Digital Transformation: A Study of how Firms Leverage Data for Insights. *Indian Journal of Information Sources and Services*, *14*(4), 29–34. https://doi.org/10.51983/ijiss-2024.14.4.05

[13] El Majdoubi, D., Khoukhi, L., Elghazi, M., & El Marraki, M. (2021). SmartMedChain: A blockchain-based privacy-preserving smart healthcare framework. *Health and Technology, 11*(6), 1373–1386.

[14] Farhood, A. S. (2023). *Analyze the Efficiency of Banking Risk Management in Banks Operating in The Local Environment Through the Application of Basel Standards in Financial Risk Management. International Academic Journal of Social Sciences, 10 (2), 39–52*. https://doi.org/10.9756/IAJSS/V10I2/IAJSS1011

[15] Hassooni, M. N. (2024). The Impact of Quantum Computing on Artificial Intelligence: An Overview. *International Academic Journal of Science and Engineering*, *11*(1), 221–228. https://doi.org/10.9756/IAJSE/V11I1/IAJSE1125

[16] Hori, Y., Claycomb, W., & Yim, K. (2012). Guest editorial: frontiers in insider threats and data leakage prevention. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, *3*(1/2).

[17] Li, X., Huang, Z., & Liu, Y. (2022). Efficient attribute-based encryption for secure data sharing in mobile health applications. *IEEE Access*, 10, 31554–31565.

[18] Mehra, P., & Patel, K. (2024). A Metrics Driven Approach to Brand Management and Brand Health Check. In Brand Management Metrics (pp. 31-47). Periodic Series in Multidisciplinary Studies.

[19] Menaka, S. R., Gokul Raj, M., Elakiya Selvan, P., Tharani Kumar, G., & Yashika, M. (2022). A Sensor based Data Analytics for Patient Monitoring Using Data Mining. *International Academic Journal of Innovative Research, 9*(1), 28–36. https://doi.org/10.9756/IAJIR/V9I1/IAJIR0905

[20] Mohammadi, K. (2017). Data analysis of digital testing for a NAND gate: electrical and business approaches. *International Academic Journal of Science and Engineering*, *4*(2), 47-58..

[21] Moravej, Z., Behravesh, V., & Bagheri, S. (2015). Optimal PMU placement for power system using binary cuckoo search algorithm. *International Academic Journal of Innovative Research*, *2*(10), 8-19.

[22] Nife, N. I., Mahmood, Z. K., Hammood, L., Ghazi, A., Al-Dawoodi, A., & Albdairi, M. (2025). Self-Supervised Learning Approach for Early Detection of Rare Neurological Disorders in MRI Data. *J. Internet Serv. Inf. Secur.*, *15*(1), 153-169. https://doi.org/10.58346/JISIS.2025.I1.010.

[23] Patnaik, D. I., Priyadarshini, P., Mishra, D., & Chaudhuri, S. D. (2025). Text to Tech: Preserving Ancient Hindu Texts in the Digital Realm. *Indian Journal of Information Sources and Services, 15*(1), 42–46. https://doi.org/10.51983/ijiss-2025.IJISS.15.1.07

[24] Pigera, S., Van Schaik, P., Renaud, K., Campbell, M., Manley, P., & Esser, P. (2025). Privacy and security in digital health contact-tracing: a narrative review. *Applied Sciences*, *15*(2), 1-32. https://doi.org/10.3390/app15020865

[25] Raman, A., Arokiasamy, A. R., Batumalai, C., Kuppusamy, M., Balakrishnan, R. D., & Louis, S. A. (2024). A Trust-based Security and Privacy Protection for Data Collection in Smart City. *J. Internet Serv. Inf. Secur.*, *14*(3), 18-28. https://doi.org/10.58346/JISIS. 2024. I3.002

[26] Rathore, M. M., Ahmad, A., Paul, A., & Islam, S. U. (2021). Secure and energy-efficient data transmission scheme for IoMT enabled healthcare systems. *IEEE Internet of Things Journal, 8*(17), 13439–13449.

[27] Shetty, V., & Kapoor, B. (2024). The Role of Participatory Governance in Strengthening Community Health Systems. *International Journal of SDG's Prospects and Breakthroughs, 2*(3), 10-12.

[28] Tran, H., & Ngoc, D. (2024). The Influence of Effective Management on Hybrid Work Styles and Employee Wellness in Healthcare Organizations. *Global Perspectives in Management*, *2*(4), 8-14.

[29] Vilpponen, H., Piirainen, A., Kallberg, M., & Mikkonen, T. (2024, November). Secondary Use of Health Data: Centralized Structure and Information Security Frameworks in Finland. In *International Conference on Software Business* (pp. 209-217). Cham: Springer Nature Switzerland. https://arxiv.org/abs/2412.06800

[30] Zhou, W., Piramuthu, S., & Zhang, Y. (2021). Privacy-Preserving Patient-Centric Data Sharing in Mobile Healthcare Systems. *IEEE Transactions on Mobile Computing, 20*(7), 2634–2646.

Authors Biography

Muntader Mhsnhasan is affiliated with the Department of Computer Techniques Engineering at the College of Technical Engineering, Islamic University of Najaf, Najaf, Iraq. His research focuses on mobile computing, data security, and ubiquitous healthcare systems. He is particularly interested in developing secure frameworks for patient data sharing in mobile and cloud-enabled environments. His work aims to enhance privacy, accessibility, and reliability in healthcare information systems through the integration of advanced security protocols and mobile technologies.

Dr.K. Venkatesh Guru is working as an Assistant Professor in School of Computing, S R M Institute of Science and Technology, Trichy, Tamil Nadu, India. He was worked as an Assistant Professor in K.S.R. College of Engineering, Tiruchengode, Tamil Nadu, India with 13 years of Experience. He completed his B.E. – CSE in K.S.R. College of Engineering, Tiruchengode and M.Tech – IT in K.S. Rangasamy College of Technology, Tiruchengode. He Completed his Ph.D in Information and Communication Engineering from Anna University, Chennai. His research area includes Wireless Sensor Networks, Cloud Computing, Artificial Intelligence and Machine Learning. He has more than 13 years of Teaching experience. He has 10 publications in National and International Journals and has three patents to his credit. He is an active member of ISTE.

S. Jeyachandran is a highly motivated and experienced marine engineer with over 40 years of distinguished service in the marine industry. A defense graduate from the Indian Navy and a Chief Engineer Certificate of Competency holder, he also holds a degree from the University of Madras. With a proven track record in team leadership, project management, and ensuring regulatory compliance, he brings deep expertise in troubleshooting, problem-solving, and maintaining Ship-in-Campus machinery. His extensive knowledge of marine engineering principles is complemented by 10 years of teaching experience. He currently oversees the Fire Laboratory, contributing both technical insight and practical training to maritime education.

Dr.A.V. Prabu is currently working as an Associate Professor in the Department of Electronics and Communication Engineering at Koneru Lakshmaiah Education Foundation (Deemed to be University), Vaddeswaram, Andhra Pradesh, India. He received his B.E. degree from Anna University, Tamil Nadu, in 2005, his M.Tech degree from Biju Patnaik University of Technology (BPUT), Odisha, and his Ph.D. from Jawaharlal Nehru Technological University, Kakinada (JNTUK), Andhra Pradesh. He has over 19 years of academic experience in the fields of Electronics and Communication Engineering and Electronics and Computer Science Engineering. His research interests include wireless sensor networks, wireless communication, healthcare technologies, and the Internet of Things (IoT).

Sandyarani Vadlamudi holds a Master of Technology in Computer Science and Engineering from Prakasam College of Engineering, JNTUK, India, in 2018. She also received her Bachelor of Engineering in Computer Science and Information Technology from Prakasam College of Engineering, JNTU, India in 2005. She is currently working as senior assistant professor in artificial intelligence and Machine Learning Department at New Horizon College of Engineering, Bengaluru, Karnataka, India. Her research includes machine learning, deep learning, Internet of Things and cyber security. She has published 7 papers and presented 2 papers in the national and international conferences. She also published a book GUARDIANS OF THE NET A COMPREHENSIVE GUIDE TO CYBER SECURITY in Prime International Publication. She is pursuing his PhD from GITAM University, Bengaluru, India. She can be contacted at email: vs.sandya@gmail.com.

Dr. Nidhi Mishra is an Assistant Professor in the Department of Computer Science and Information Technology at Kalinga University, Raipur, India. Her areas of expertise include artificial intelligence, machine learning, and data analytics. She is actively involved in academic research, curriculum development, and student mentorship. Dr. Mishra has published in reputed national and international journals and conferences, with a focus on applying intelligent computing techniques to solve real-world problems in diverse domains.