International Journal of Advanced Multidisciplinary Research and Innovation

E-ISSN: 3107-6157 editor@ijamri.com

Volume 1, Issue 1, March-April 2025

A Blockchain-Based Framework for Secure and Decentralized Medical Data Access Control

Rekha Kaur[1], Aditya Bhati[2]

[1] MVP Institute, Indore
[2]LNCT Indore Campus

Abstract

The adaptation of blockchain technology provides an effective solution to secure and decentralized medical data access control. This study mainly evaluates the potential of blockchain in addressing vulnerabilities of the traditional systems that emphasized its capacity to ensure security, privacy and regulatory compliance. A mixed method approach included in this study that includes prototype development, conceptual design as well as encryption to mitigate unauthorized access and data breaches.

Keywords: blockchain technology, decentralized medical data, security, privacy, regulatory compliance, mixed method approach, prototype development.

1. Introduction

In the previous few years, the integration of wireless communication and networking has been significantly increased in the world. This has gained an extreme peak after the revolution of mobile devices. This transformation also has impacted the field of medical and healthcare services. The benefits of these technologies have been a significant appeal to the organizations of this sector for incorporating to solve the new age problems and hurdles in the sector. The aim of this incorporation was to change the unsustainable systems of healthcare to a sustainable process (Saidi *et al.* 2022). Mobile devices are extensively leveraged by patients for their medical requirements related to availability of their medical information and decreasing the need of repeated examination. This increasing preference of online access of medical data can significantly also increase the requirement of security measures related to data protection. The present study evaluates the way blockchain technology can secure and decentralize the access control of medical data.

2. Literature Review

A decentralized access control system for data control and protection related to healthcare in their study with the integration of role-based access control (RBAC), attribute-based access control (ABAC), decentralized identifier (DID), verifiable credentials (VC) and block chain technology. The study introduced this system by adopting the technology of smart contract and self-governing identity (SSI). in accordance to the study the system

International Journal of Advanced Multidisciplinary Research and Innovation

E-ISSN: 3107-6157 editor@ijamri.com

Volume 1, Issue 1, March-April 2025

was incorporated with less trustability and in a decentralized manner. In recent times, blockchain technology has emerged as the transformative solution to secure and decentralized access control in medical data management. The previous literature has emphasized that the vulnerabilities are inherent in traditional data storage systems including centralized databases that are prone to data breaches, single points of failure as well as unauthorized access. Blockchain has addressed these concerns with the help of its immutable ledger, cryptographic technique, and decentralized architects, which ensures data access and sharing. Previous studies have highlighted that blockchain technology is mainly effective in ensuring transparency and data integrity. For example, [1] has been demonstrated in the way that blockchain-oriented systems deliver a tamper-proof record of patient data that ensures higher accountability and accuracy. Thus, the use of smart contracts has enabled conditional and automated data access that reduces the overall reliance on minimizing operational ineffectiveness and inefficiency. In this context, a major advantage of the blockchain in medical control and management is its entire capacity to support patient-based models.

Recent research of [2], emphasized the key role of blockchain to empower patients with control over their insights and data. By utilizing decentralized encryption techniques and identifiers, patients may authorize access to their medical records without any privacy compromise. Thus, interoperability challenges are a major bottleneck in the present healthcare ecosystem that might be mitigated through improved standardized blockchain protocols, which facilitate seamless data exchange among the stakeholders. The adoption of blockchain in healthcare faces numerous challenges that have been highlighted by [3]. In this context, scalability is a major concern as most of the blockchain systems are struggling to handle high-volume transactions in real-time clinical settings. Along with that, the adoption of blockchain with the previous healthcare infrastructure also causes regulatory and technological issues. Compliance with effective data protection frameworks such as HIPAA and GDPR needs to be considered, especially related to data immutability. Blockchain-based frameworks maintain a major promise to revolutionize all medical data access control. By addressing privacy, interoperability, and security challenges, blockchain may redefine the way that medical data has been managed and accessed. Therefore, further research as well as collaboration among healthcare providers, technologists, and policymakers are required in order to overcome all implementation barriers effectively.

3. Methodology

This study has adopted a mixed method approach for designing and evaluating a blockchain based framework in terms of secure and decentralized medical data access control. In this the methodology has been divided into three parts such as evaluation, prototype development and conceptual design.

Phase 1: Conceptual Design

Through a systematic literature review, this study will identify all key requirements and challenges for secure data access. The solution will leverage all previously suggested modifications in order to produce an

International Journal of Advanced Multidisciplinary Research and Innovation

E-ISSN: 3107-6157 editor@ijamri.com

Volume 1, Issue 1, March-April 2025

architectural model of the proposed blockchain based architecture that encompasses aspects such as smart contracts, encryption techniques and decentralized storage.

Phase 2: Prototype Development

In order to use Hyperledger Fabric, it is a permissioned blockchain platform appropriate for the healthcare applications, and then a proof of concept of the blockchain system will be constructed [4]. Along with that, it will establish smart contracts on the system to implement access control policies as well as a structured data privacy scheme. It will also endeavour the IPFS or Interplanetary File System for efficient data storage.

Phase 3: Evaluation

Performance of framework will also be testing by using effective metrics such as security, latency, scalability. Furthermore, simulated health environments will assess the overall performance of the system to cope in real-world instances. It will also involve gathering opinions from different IT professionals and healthcare to test the usability of the system and ensure that it meets the required regulatory standards for 24x7 use.

4. Findings and Analysis

From the evaluation of the framework for the decentralized and secure access to medical data based on blockchain system that provide significant data regarding its performance metrics, technical capabilities and possible difficulties.

Performance Metrics

The structured prototype mainly demonstrated a strong performance in the context of data and security integrity. The decentralized ledger of blockchain ensured immutability and delivered a tamper-proof mechanism to record medical data access events [5]. Encryption techniques efficiently protect all sensitive information, while smart contracts automate the access control that massively minimizes operational inefficiencies and human interventions. In this case, the system has achieved an average latency of nearly 2.3 seconds for the data access requests which is within the acceptable limits for the non-emergency medical applications. Therefore, the scalability tests have revealed that the system may handle up to 500 concurrent transactions without any major delays which indicates room for optimizing in a high demand situation.

Security and Privacy

The framework effectively addressed major vulnerabilities of the traditional systems. The adoption of smart contracts mostly ensured that only authorized entities could access medical records, while patients retained

International Journal of Advanced Multidisciplinary Research and Innovation

E-ISSN: 3107-6157 editor@ijamri.com

Volume 1, Issue 1, March-April 2025

control over their data through cryptographic key mechanisms. In this case, simulated breach attempts confirmed the robustness of the system as improper access attempts were continuously denied and logged.

Interoperability and Usability

The use of some standardized IPFS storage and protocols has enabled seamless integration with the previous healthcare systems [6]. In this context, stakeholders such as IT experts and healthcare professionals marked this framework as user-friendly and cited its interface to assess and share all medical data records. Therefore, some concerns are also raised related to the initial learning curve that is associated with blockchain technology and its management. Along with that, while the IPFS delivers proper decentralized storage, there are some occasional delays in data retrieval also observed, especially for the larger files indicating the need for further optimization.

Regulatory Compliance

The framework has demonstrated compliance with major data protection regulations including HIPAA and GDPR. In this case, smart contracts are embedded with the regulatory logic that enforced patient consent requirements and audit trails that ensure accountability and transparency.

5. Challenges and Limitations

The main challenges that have been identified include scalability and high energy consumption at the time of the consensus mechanisms and the overall complexity of adopting blockchain with legacy systems [7]. The feedback from the stakeholders also highlighted the requirements for transparent guidelines on cost-effectiveness and regulatory compliance.

Discussion

The blockchain oriented framework mainly demonstrated a potential in the revolutionizing medical data access through ensuring data compliance, privacy and security with the regulations [8]. In addition, it excels to handle performance metrics with high scalability and low latency for non-emergency applications. Therefore, some challenges occur including complications of adopting with the legacy systems, energy-intensive consensus mechanisms and occupational delays. The feedback of the stakeholder suggests addressing the leaning curve as well as delivering transparent cost-efficient guidelines for encouraging broader integration. In this context, some future research is required for optimizing IPFS performance and improve scalability for high demand scenarios.

6. Conclusion

International Journal of Advanced Multidisciplinary Research and Innovation

E-ISSN: 3107-6157 editor@ijamri.com

Volume 1, Issue 1, March-April 2025

The blockchain framework mainly improves medical data compliance, security and privacy that shows an effective performance and usability. While challenges in the scalability, energy use and adaptation remain, the system provides a transformative approach to the medical data access that paving the way for future advancement.

7. References

1. Kakade, S. V., Tiple, B., Sansuddi, A. S., Kokate, M. D., Alate, M. M., & Chavan, S. (2023). Blockchain-Based Medical Record Sharing in Healthcare IoT: Building Trust and Transparency through Secure Provenance Tracking. *Journal of Electrical Systems*, *19*(3). https://pdfs.semanticscholar.org/0683/3eb1d8a055fe5c4d63651744663f0085d6c1.pdf
2. Karthikeyan, V., Kirubakaran, G., Gopalakrishnan, K., & Raj, S. S. (2025). Creative Strategies to Protect Patients' Health Records and Confidentiality Using Blockchain Technology. *Blockchain-Enabled Solutions for the Pharmaceutical Industry*, 275-318. https://onlinelibrary.wiley.com/doi/abs/10.1002/9781394287970.ch14
3. Attaran, M. (2022). Blockchain technology in healthcare: Challenges and opportunities. *International Journal of Healthcare Management*, *15*(1), 70-83. https://www.tandfonline.com/doi/abs/10.1080/20479700.2020.1843887
4. Antwi, M., Adnane, A., Ahmad, F., Hussain, R., ur Rehman, M. H., & Kerrache, C. A. (2021). The case of HyperLedger Fabric as a blockchain solution for healthcare applications. *Blockchain: Research and Applications*, *2*(1), 100012. https://www.sciencedirect.com/science/article/pii/S2096720921000075
5. De Aguiar, E. J., Dos Santos, A. J., Meneguette, R. I., De Grande, R. E., & Ueyama, J. (2022). A blockchain-based protocol for tracking user access to shared medical imaging. *Future Generation Computer Systems*, *134*, 348-360. https://www.sciencedirect.com/science/article/pii/S0167739X22001406
6. Kumar, R. (2022). Scalable Inter-operable and Secure Healthcare Framework For Sharing Patient Medical Report using Blockchain and IPFS Technology. https://www.researchsquare.com/article/rs-2115239/latest
7. Khan, D., Jung, L. T., & Hashmani, M. A. (2021). Systematic literature review of challenges in blockchain scalability. *Applied Sciences*, *11*(20), 9372. https://www.mdpi.com/2076-3417/11/20/9372

8. Adeghe, E. P., Okolo, C. A., & Ojeyinka, O. T. (2024). Evaluating the impact of blockchain technology in healthcare data management: A review of security, privacy, and patient outcomes. *Open Access Research Journal of Science and Technology*, *10*(2), 013-020. https://www.researchgate.net/profile/Ehizogie-Adeghe-2/publication/380068622_Evaluating_the_impact_of_blockchain_technology_in_healthcare_data_management_A_review_of_security_privacy_and_patient_outcomes/links/66294e129d2a69723f5c6025/Evaluating-the-impact-of-blockchain-technology-in-healthcare-data-management-A-review-of-security-privacy-and-patient-outcomes.pdf