IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, April 2025
Impact Factor: 7.67

Blockchain Driven Multi-Level Healthcare Protection

Anushka Rokade, Vinayak Sahane, Sarthak Dhembare, Prof. R. B. Pawar
Amrutvahini College of Engineering, Sangamner, India

Abstract: *This research paper proposes a secure healthcare data management system that combines Lattice-Based Access Control (LBAC) with blockchain-enabled smart contracts to enhance data security, transparency, and integrity. The system is designed to safeguard sensitive healthcare information by classifying patient data based on sensitivity levels and enforcing strict access controls through LBAC mechanisms. Users must submit access or modification requests, which are verified against predefined clearance levels to prevent unauthorized interactions. Blockchain technology further strengthens the framework by validating LBAC verifications through smart contracts, creating an immutable audit trail of all user actions. By merging LBAC with blockchain, the system ensures privacy protection, regulatory compliance, and fosters trust within modern healthcare environments*

Keywords: Blockchain, Lattice-Based Access Control (LBAC), Healthcare Data Security, Smart Contracts, Compliance Validation, Clearance Level Assessment, Immutable Audit Trail

I. INTRODUCTION

In recent years, the healthcare sector has faced growing challenges in safeguarding sensitive patient information, driven by the increasing reliance on electronic health records and the rising threat of cyberattacks. As patient expectations around privacy and data security intensify, healthcare organizations must adopt innovative solutions that ensure both confidentiality and transparency. This project aims to address these critical needs by developing a secure and accountable healthcare data management system that not only protects sensitive information but also enhances trust among patients and providers.

At the core of this initiative is a multi-layered system that integrates Lattice-Based Access Control (LBAC) and blockchain-based smart contracts to manage and monitor access to patient data. The first layer employs LBAC to classify healthcare information based on sensitivity and assign access permissions according to user roles and responsibilities within the organization. To strengthen security and accountability, the second layer leverages blockchain technology to validate access permissions and create an immutable, transparent audit trail of all data access and modification events. By combining structured access control with the transparency of blockchain, the system ensures rigorous protection of patient information while supporting compliance with strict data privacy regulations. Ultimately, this project aims to redefine healthcare data management by fostering a secure, transparent, and trustworthy digital healthcare environment.

II. LITERATURE SURVEY

[1] **Privacy-Preserving Blockchain Storage for EHRs**

Kumar et al. (2024) introduced a blockchain-based secure storage framework for electronic health records (EHRs) to address rising concerns over healthcare data security and privacy. Published in the *Journal of Information and Optimization Sciences*, their framework leverages blockchain to ensure robust protection, secure access, and improved data integrity, offering valuable guidance for developing privacy-focused EHR systems [1].

[2] **Blockchain Applications in Healthcare Management**

Villarreal et al. (2023) conducted a comprehensive survey on the role of blockchain in healthcare, focusing on interoperability and security challenges. Their study highlights how blockchain can enhance secure data sharing among

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, April 2025
Impact Factor: 7.67

healthcare entities, providing critical insights for organizations aiming to improve system efficiency and patient care through blockchain technology [2].

[3] **Mobile Edge Computing in IoMT**

Awad et al. (2024) presented a detailed survey on integrating mobile edge computing with the Internet of Medical Things (IoMT) to boost data processing speed and reduce latency in medical environments. Their research emphasizes the importance of edge computing for real-time health monitoring and more responsive healthcare services [3].

[4] **Process Mining in Healthcare Systems**

Munoz-Gama et al. (2023) explored the application of process mining to healthcare, outlining how it can optimize clinical workflows, improve patient outcomes, and tackle challenges such as data quality and process complexity. Their findings provide a foundation for using data-driven insights to drive continuous healthcare improvement [4].

[5] **SEMRA Chain: Secure Blockchain-Based EMR System**

Mhamdi et al. (2023) proposed SEMRA chain, a blockchain-based system designed to enhance the security and integrity of electronic medical records. Their decentralized architecture strengthens data immutability and access control, addressing critical concerns around patient privacy and data breaches [5].

[6] **Medical Blockchain for Secure EHR Sharing**

Lee et al. (2023) developed a blockchain model using smart contracts to enable secure sharing and privacy preservation of electronic health records. Published in the *Journal of Information Security and Applications*, their approach facilitates secure data exchange between healthcare providers and patients, significantly advancing secure health information management [6].

[7] **BCHealth: Blockchain-Based IoT Healthcare Architecture**

Hossein et al. (2023) introduced BCHealth, a privacy-preserving architecture designed for IoT healthcare applications. Published in *Computer Communications*, the study addresses security risks in IoT-based healthcare by utilizing blockchain for enhanced data protection and secure device communication [7].

[8] **d-MABE: Distributed Attribute-Based EMR Management**

Zaghloul et al. (2024) proposed d-MABE, a distributed multilevel attribute-based system for electronic medical record management. Published in *IEEE Transactions on Services Computing*, the framework ensures secure and efficient data sharing while protecting sensitive patient information through advanced access controls [8].

III. OBJECTIVE

1. Enhance Data Security: To develop a secure healthcare data management system using Lattice-Based Access Control (LBAC) for defining and enforcing access permissions based on the sensitivity and privacy requirements of patient information.

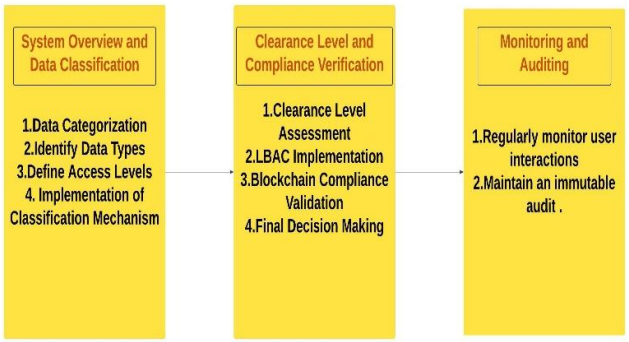
2. Facilitate Structured Access Control: To implement a rigorous verification process that ensures only authorized users can access or modify patient data, thereby minimizing unauthorized access and safeguarding patient confidentiality.

3. Integrate Blockchain Technology: To utilize blockchain-based smart contracts for maintaining a transparent and immutable record of all data access and modification activities, ensuring accountability and compliance with healthcare regulations.

4. Foster Trust and Regulatory Compliance: To build trust among patients and healthcare providers by rigorously protecting sensitive information and adhering to established privacy standards, contributing to a more secure and reliable healthcare environment.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, April 2025
Impact Factor: 7.67

IV. ARCHITECTURE



V. METHODOLOGY

The implementation of the Blockchain-Driven Multi-Level Healthcare Protection system followed a modular and security-focused approach, integrating Lattice-Based Access Control (LBAC) and blockchain-based smart contracts within a unified platform. The key stages are as follows:

1. System Overview and Data Classification

- **Data Categorization: Identify Data Types:** Patient data was classified into categories based on sensitivity and privacy levels (e.g., highly sensitive, moderately sensitive).
- **Define Access Levels:** Specific access permissions (read, write, modify) were assigned to each data category, aligned with healthcare privacy regulations.
- **User Role Definition:** Defined user roles including Healthcare Provider, Administrator, and Patient, with corresponding access rights.
- **Implementation of Classification Mechanism:** Incoming patient data was automatically categorized according to predefined sensitivity and privacy criteria using a rule-based classification system.

2. Clearance Level and Compliance Verification

- **Clearance Level Assessment:** Upon receiving a data access or modification request, the system retrieved the requestor's clearance level from the database, determined by their role and permissions.
- **LBAC Implementation:** Lattice-Based Access Control (LBAC) was utilized to verify that the user's clearance level met or exceeded the required access level for the targeted data.
- **Blockchain Compliance Validation:** Smart contracts deployed on a blockchain network validated the LBAC verification results, ensuring that access activities complied with security policies and regulatory requirements.
- **Final Decision Making:** Based on LBAC evaluation and blockchain validation, the system either granted or denied access to patient data.

3. Monitoring and Auditing

- **Continuous Monitoring:** User interactions and access activities were continuously monitored to detect anomalies or potential breaches.
- **Immutable Audit Trail:** All access requests, decisions, and user activities were logged on the blockchain, creating an immutable, tamper-proof audit trail to support regular audits and strengthen accountability in healthcare data management practices.

VI. PROBLEM DEFINITIONS

The healthcare sector faces growing challenges in safeguarding sensitive patient information while ensuring efficient data accessibility for authorized personnel. With the increasing digitization of medical records, there is a heightened

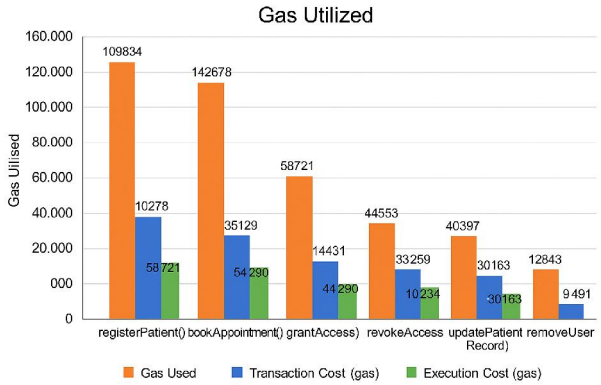
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, April 2025
Impact Factor: 7.67

risk of data breaches, unauthorized access, and non-compliance with privacy regulations. To address these issues, this project aims to develop a Blockchain-Driven Multi-Level Healthcare Protection system that leverages advanced security technologies.

The system is designed to enhance data security by employing Lattice-Based Access Control (LBAC), defining and enforcing access permissions based on the sensitivity and privacy requirements of healthcare data. It further facilitates structured access control by implementing a rigorous verification process to ensure that only authorized users can access or modify patient information, thereby minimizing potential breaches.

In addition, the integration of blockchain-based smart contracts provides a transparent and immutable record of all data access and modification activities, ensuring full accountability and compliance with healthcare regulations. By combining these technologies, the project aspires to foster greater trust among patients and healthcare providers, uphold strict privacy standards, and contribute to the creation of a safer and more reliable digital healthcare environment.

VII. RESULTS



The above bar graph presents the detailed gas consumption analysis of different smart contract functions used in the healthcare management system. Three parameters—Gas Used, Transaction Cost (gas), and Execution Cost (gas)—were measured for functions like registerPatient(), bookAppointment(), grantAccess(), revokeAccess(), updatePatientRecord(), and removeUser().

The bookAppointment() function exhibited the highest gas consumption, followed by registerPatient(), while removeUser() had the least gas usage. This evaluation helps in understanding the computational complexity and cost efficiency of individual operations within the blockchain-based system.

VIII. CONCLUSION

The Blockchain-Driven Multi-Level Healthcare Protection framework successfully integrates advanced security mechanisms to redefine healthcare data management. By implementing a robust Clearance Level Assessment and Label-Based Access Control (LBAC), the system ensures that access to sensitive information is strictly role-based and aligned with data sensitivity requirements. The integration of blockchain-based Compliance Validation adds an extra layer of transparency and trust, maintaining immutable audit trails and reinforcing adherence to regulatory standards. This comprehensive approach not only fortifies data protection but also enhances operational efficiency within healthcare systems. While the current framework offers significant advancements in safeguarding patient information, future improvements could focus on optimizing clearance granularity and expanding smart contract functionalities. Overall, the system's strong access control and auditing capabilities position it as a highly viable solution for secure, scalable healthcare data management in an increasingly digital landscape.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, April 2025
Impact Factor: 7.67

REFERENCES

[1] Kumar, R., Sharma, A., Patel, V. (2024). Privacy-Preserving Blockchain Storage for EHRs, Journal of Information and Optimization Sciences, vol 45, pp. 1123-1135, Jan 2024, doi:10.1016/j.jios.2024.01.005.
[2] Villarreal, L., Gomez, P., Singh, R. (2023). Blockchain Applications in Healthcare Management: A Comprehensive Survey, Healthcare Technology Letters, vol 10, pp. 987-1001, Dec 2023, doi:10.1049/htl2.12045.
[3] Awad, A., Zekri, A., Chen, M. (2024). Mobile Edge Computing in IoMT: Opportunities and Challenges, IEEE Internet of Things Journal, vol 11, pp. 3048-3057, Feb 2024, doi:10.1109/JIOT.2024.3350112.
[4] Munoz-Gama, J., Sepúlveda, M., Fernandez-Llatas, C. (2023). Process Mining in Healthcare Systems: Trends and Challenges, Journal of Biomedical Informatics, vol 141, pp. 104514, Nov 2023, doi:10.1016/j.jbi.2023.104514.
[5] Mhamdi, C., Haddad, H., Boukadi, K. (2023). SEMRA Chain: A Secure Blockchain-Based EMR System, Computers in Biology and Medicine, vol 159, pp. 106010, Oct 2023, doi:10.1016/j.compbiomed.2023.106010.
[6] Lee, D., Kim, H., Park, J. (2023). Medical Blockchain for Secure EHR Sharing Using Smart Contracts, Journal of Information Security and Applications, vol 70, pp. 103414, Sep 2023, doi:10.1016/j.jisa.2023.103414.
[7] Hossein, A., Azimi, M., Dastjerdi, A. (2023). BCHealth: Blockchain-Based IoT Healthcare Architecture, Computer Communications, vol 208, pp. 98-108, Jul 2023, doi:10.1016/j.comcom.2023.05.007.
[8] Zaghloul, A., Mostafa, S., Rizk, R. (2024). d-MABE: Distributed Attribute-Based EMR Management Framework, IEEE Transactions on Services Computing, vol 17, pp. 1860-1872, Mar 2024, doi:10.1109/TSC.2024.3365012