Global Journal of Engineering Innovations & Interdisciplinary Research

Original Article

Blockchain Driven Security Frame Work For Healthcare Record Management

V.K.Pavani, Beesu Lakshmidevi, Baine Hindu, P Dhanush Kumar Reddy, Malle Lokesh, Geedi Jayanth.

Department of Computer Science and Engineering, Gates Institute of Technology, Andhra Pradesh, India.

Abstract

Healthcare data security and privacy are critical concerns in modern medical systems. This paper presents a Blockchain Driven Security Framework for Healthcare Record Management that leverages advanced cryptographic techniques and decentralized architecture to ensure secure and tamper-proof storage of patient records. Data is protected using SHA-256 hashing and digital signatures, preventing unauthorized access and modification. The system implements role-based access control, enabling patients, doctors, and administrators to securely access and share medical data. Cloud integration enhances scalability and availability, while an intrusion detection mechanism identifies potential security threats. The proposed framework ensures transparency, traceability, and improved interoperability, ultimately strengthening data security, reducing breaches, and enhancing trust in healthcare systems.

Correspondence

V.K.Pavani

Department of Computer Science and Engineering, Gates Institute of Technology, Andhra Pradesh, India.

- Received Date: 11 Feb 2026
- Accepted Date: 02 Apr 2026
- Publication Date: 25 Apr 2026

Keywords

Blockchain, Healthcare Security, SHA-256, Digital Signatures, Access Control, Data Privacy, Intrusion Detection

Introduction

Healthcare data security and privacy have become critical concerns in modern medical systems due to the rapid digitization of patient records. Traditional healthcare systems rely on centralized databases, which are highly vulnerable to cyberattacks, data breaches, and unauthorized access. These systems lack transparency, are prone to single points of failure, and often fail to provide patients with full control over their medical data.

With the increasing demand for secure and efficient data management, there is a need for advanced solutions that ensure confidentiality, integrity, and accessibility of healthcare records. Blockchain technology has emerged as a powerful tool to address these challenges due to its decentralized, immutable, and transparent nature. It enables secure data storage and sharing without relying on a central authority.

The proposed Blockchain Driven Security Framework for Healthcare Record Management integrates blockchain technology with cryptographic techniques such as SHA-256 hashing and digital signatures to secure patient data. The system implements role-based access control, allowing only authorized users such as patients, doctors, and administrators to access specific information.

Additionally, the framework incorporates intrusion detection mechanisms to identify unauthorized access attempts and ensure system reliability. By combining decentralization, encryption, and secure authentication, the proposed system enhances data privacy, improves interoperability, and reduces the risk of data breaches, making it a robust solution for modern healthcare environments.

Related Work

Several research studies and existing systems have focused on improving healthcare data security using various technologies such as centralized databases, cloud-based storage, and encryption techniques. Traditional systems rely heavily on centralized architectures, which are easier to manage but highly susceptible to data breaches, single points of failure, and unauthorized access.

Cloud-based healthcare systems have improved data availability and scalability; however, they still face significant challenges related to data privacy, trust, and security. Although encryption techniques are used to protect sensitive data, these systems depend on third-party service providers, which raises concerns about data ownership and control.

Recent advancements have explored the use of blockchain technology in healthcare for secure data sharing and management. Blockchain-based systems provide immutability, transparency, and decentralized control, reducing the risks associated with centralized systems. Some studies have implemented blockchain for Electronic Health Records (EHR), ensuring secure and tamper-proof data storage.

However, many existing solutions lack comprehensive security mechanisms such as intrusion detection, fine- grained access control, and efficient system scalability. The proposed system addresses these limitations by integrating blockchain with advanced

Citation: Pavani VK, Beesu L, Baine H, Reddy PDK, Malle L, Geedi J. Blockchain Driven Security Frame Work For Healthcare Record Management. GJEIIR. 2026;6(4):234.

cryptographic techniques, role-based access control, and intrusion detection features, thereby providing a more secure and efficient healthcare data management solution.

Proposed Methodology

The proposed system is designed as a multi-layered architecture that integrates frontend interfaces, backend processing, blockchain technology, and database management to ensure secure and efficient healthcare record management. The system leverages blockchain along with advanced cryptographic techniques to provide a tamper-proof and decentralized platform for storing and sharing medical data.

The framework uses RESTful APIs for seamless communication between frontend and backend components. All data transactions are secured using encryption mechanisms such as SHA-256 hashing and digital signatures to prevent unauthorized access and data manipulation. The blockchain network maintains a distributed ledger where each transaction is recorded immutably, ensuring transparency and traceability.

The backend system, developed using Spring Boot, processes requests in real time and enforces role-based access control. Only authorized users such as patients, doctors, and administrators are allowed to access specific healthcare data. The system is designed to handle multiple users simultaneously with high efficiency and scalability.

Additionally, the system incorporates an intrusion detection mechanism to monitor suspicious activities and prevent security breaches. Error handling and validation techniques are implemented to ensure system reliability even in cases of network failures or unexpected inputs.

System Workflow

The process begins when a user logs into the system using valid credentials through a web interface. Once authenticated, the user can perform actions such as uploading, accessing, or updating medical records.

When a transaction is initiated, the data is encrypted and converted into a secure hash using SHA-256. This hashed data is then stored in the blockchain as a new block. Each block is linked to the previous one, forming a secure and immutable chain.

The system verifies user permissions using role-based access control before granting access to the requested data. If the user is authorized, access is granted; otherwise, the request is denied and logged for further analysis.

All transactions are recorded in the system, ensuring full transparency and traceability of healthcare data operations.

System Architecture

The system architecture consists of three primary layers:

- Frontend Layer: Developed using HTML, CSS, and JavaScript, this layer provides an interactive interface for users to register, log in, and manage healthcare records.
- Backend Layer: Implemented using Spring Boot, this layer handles business logic, authentication, blockchain interaction, and secure data processing.
- Database & Blockchain Layer: MySQL is used for storing user details and metadata, while blockchain is used for secure, decentralized storage of hashed healthcare records and transaction logs.

Modules Description

- Patient Management Module: Handles patient registration, login, and medical record uploads.
- Doctor Module: Allows doctors to access, update, and manage patient records securely.
- Admin Module: Manages system users, monitors activities, and controls permissions.
- Blockchain Module: Ensures secure storage of records using hashing and block creation.
- Access Control Module: Implements role-based permissions for secure data access.
- Intrusion Detection Module: Monitors and detects unauthorized access attempts.
- Logging Module: Records all system activities for auditing and tracking purposes.

Advantages of Proposed System

The integration of blockchain technology ensures that healthcare data is secure, immutable, and tamper-proof. Unlike traditional systems, the proposed framework eliminates single points of failure through decentralization. The use of cryptographic techniques enhances data privacy and integrity, while role-based access control ensures that only authorized users can access sensitive information.

Additionally, the system provides transparency, traceability, and efficient data sharing among healthcare stakeholders. The inclusion of intrusion detection further strengthens system security, making it a reliable and scalable solution for modern healthcare environments.

Results And Discussion

The proposed blockchain-based healthcare system was evaluated under various conditions to analyze its performance, security, and reliability. The system demonstrated efficient handling of healthcare data transactions with high accuracy and minimal processing delay.

During testing, the blockchain module successfully ensured data integrity by generating unique SHA-256 hashes for each transaction. Any attempt to modify stored data resulted in hash mismatches, proving the system's capability to detect tampering. The backend system efficiently processed user requests, including data upload, retrieval, and verification, ensuring a smooth and responsive user experience.

The system also handled multiple user requests simultaneously without significant performance degradation, showcasing its scalability. Role-based access control effectively restricted unauthorized users from accessing sensitive patient data. Additionally, the intrusion detection mechanism successfully identified suspicious activities and logged them for further analysis.

Compared to traditional centralized systems, the proposed framework significantly reduces the risk of data breaches and unauthorized access. The use of blockchain enhances transparency and traceability, as all transactions are securely recorded and can be verified at any time.

Future Work

The proposed system can be further enhanced by integrating advanced technologies to improve functionality and user experience. One major improvement is the development of a mobile application, enabling users to access healthcare services more conveniently and efficiently.

Integration with Internet of Things (IoT) devices such as wearable health monitors can allow real-time data collection and automatic updates to patient records. Artificial Intelligence (AI) techniques can be incorporated to analyze patient data,

predict health conditions, and detect anomalies in system usage.

The system can also be extended to support large-scale blockchain networks for improved scalability and interoperability among multiple healthcare organizations. Cloud integration can further enhance data availability, backup, and remote access capabilities.

Additionally, advanced security mechanisms such as multi-factor authentication and biometric verification can be implemented to strengthen user authentication. Future improvements may also include optimizing blockchain performance to reduce latency and energy consumption, making the system more efficient for real-world deployment.

System Design

The system design follows a modular and layered architecture, ensuring flexibility, scalability, and ease of maintenance. Each component is designed to perform specific functions and interact with other modules through secure and well-defined interfaces.

The frontend layer is developed using HTML, CSS, and JavaScript, providing a user-friendly interface for patients, doctors, and administrators. It allows users to register, log in, upload medical records, and access data securely.

The backend layer, implemented using Spring Boot, acts as the core of the system. It handles user authentication, business logic, blockchain interaction, and secure API communication. The backend also enforces role-based access control and processes all requests efficiently.

The database and blockchain layer combines MySQL and blockchain technology. MySQL stores user information and metadata, while blockchain ensures secure and immutable storage of healthcare records. Each transaction is encrypted and stored as a block, maintaining data integrity and traceability.

Security is a key aspect of the system design. Techniques such as SHA-256 hashing, digital signatures, secure APIs, and authentication tokens are used to protect sensitive healthcare data. The system also includes logging and monitoring mechanisms to track all activities and detect potential security threats.

Overall, the modular design ensures that the system is robust, scalable, and capable of meeting the security requirements of modern healthcare applications.

Security

Security is a fundamental aspect of the proposed blockchain-based healthcare system. Multiple layers of security are implemented to ensure maximum protection of sensitive medical data against unauthorized access and cyber threats.

The first layer involves user authentication, where credentials are securely verified using authentication mechanisms such as tokens and encrypted passwords. The second layer is role-based access control, ensuring that only authorized users (patients, doctors, and administrators) can access specific data based on their roles.

A key security feature of the system is the use of cryptographic techniques, including SHA-256 hashing and digital signatures. These techniques ensure data integrity by converting healthcare records into unique hash values, making it impossible to alter data without detection.

The system also utilizes secure communication protocols (HTTPS) to protect data during transmission between the frontend and backend. Additionally, blockchain technology provides decentralization and immutability, eliminating single points of failure and ensuring that once data is stored, it cannot be modified.

An intrusion detection mechanism is incorporated to monitor system activities and identify suspicious behavior. All transactions and access attempts are recorded in logs, enabling administrators to track activities and respond to potential security threats effectively.

These combined security measures make the system highly reliable, secure, and suitable for managing sensitive healthcare information.

Conclusion

The proposed Blockchain Driven Security Framework for Healthcare Record Management presents an advanced solution for securing and managing healthcare data in modern digital environments. By integrating blockchain technology with cryptographic techniques, the system ensures data integrity, privacy, and transparency.

Unlike traditional centralized systems, the proposed framework eliminates the risk of single points of failure and significantly reduces the chances of data breaches and unauthorized access. The implementation of role- based access control and secure authentication mechanisms ensures that only authorized users can access sensitive medical records.

The system also enhances trust among healthcare stakeholders by providing transparency and traceability of all transactions. Its scalable architecture and efficient performance make it suitable for real-world healthcare applications.

Overall, the proposed system offers a secure, reliable, and efficient approach to healthcare record management. With future enhancements such as AI integration and advanced analytics, it has the potential to further improve healthcare services and data security, making it a valuable contribution to the field of healthcare technology.

References

1. Choe, J., Lee, S.M., Do, K.H., Lee, G., Lee, J.G., Lee, S.M. and Seo, J.B., 2019. Deep learning–based image conversion of CT reconstruction kernels improves radiomics reproducibility for pulmonary nodules or masses. Radiology, 292(2), pp.365-373.
2. Kermany, D.S., Goldbaum, M., Cai, W., Valentim, C.C., Liang, H., Baxter, S.L., McKeown, A., Yang, G., Wu, X., Yan, F. and Dong, J., 2018. Identifying medical diagnoses and treatable diseases by image- based deep learning. Cell, 172(5), pp.1122-1131.
3. Negassi, M., Suarez-Ibarrola, R., Hein, S., Miernik, A. and Reiterer, A., 2020. Application of artificial neural networks for automated analysis of cystoscopic images: a review of the current status and future prospects. World Journal of Urology, pp.1-10.
4. Gulshan, V., Peng, L., Coram, M., Stumpe, M.C., Wu, D., Narayanaswamy, A., Venugopalan, S., Widner, K., Madams, T., Cuadros, J. and Kim, R., 2016. Development and validation of a deep learning algorithm for detection of diabetic retinopathy in retinal fundus photographs. Jama, 316(22), pp.2402-2410.
5. Tandon, A., Dhir, A., Islam, N. and Mäntymäki, M., 2020. Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. Computers in Industry, 122, p.103290. [6]Yang, Q., Liu, Y., Chen, T. and Tong, Y., 2019. Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology (TIST), 10(2), pp.1-19.
6. Kairouz, P., McMahan, H.B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A.N., Bonawitz, K., Charles, Z., Cormode, G., Cummings, R. and d'Oliveira, R.G., 2019. Advances and open problems in federated learning. arXiv preprint arXiv:1912.04977.
7. Li, W., Milletarì, F., Xu, D., Rieke, N., Hancox, J., Zhu, W., Baust, M., Cheng, Y., Ourselin, S., Cardoso,
8. M.J. and Feng, A., 2019, October. Privacy-preserving federated brain tumour segmentation. In International Workshop on Machine Learning in Medical Imaging (pp. 133-141). Springer,

Cham. [9]Sheller, M.J., Reina, G.A., Edwards, B., Martin, J. and Bakas, S., 2018, September. Multi-institutional deep learning modeling without sharing patient data: A feasibility study on brain tumor segmentation. In International MICCAI Brainlesion Workshop (pp. 92-104). Springer, Cham.

9. Sekeroglu, B. and Ozsahin, I., 2020. <? covid19?> Detection of COVID-19 from Chest X-Ray Images Using Convolutional Neural Networks. SLAS TECHNOLOGY: Translating Life Sciences Innovation, p.2472630320958376.
10. Jain, R., Gupta, M., Taneja, S. and Hemanth, D.J., 2020. Deep learning based detection and analysis of COVID-19 on chest X-ray images. Applied Intelligence, pp.1-11.
11. Ozturk, T., Talo, M., Yildirim, E.A., Baloglu, U.B., Yildirim, O. and Acharya, U.R., 2020. Automated detection of COVID-19 cases using deep neural networks with X-ray images. Computers in Biology and Medicine, p.103792.
12. Patel, V., 2019. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Health informatics journal, 25(4), pp.1398-1411.
13. Linn, L.A. and Koo, M.B., 2016. Blockchain for health data and its potential use in health it and health care related research. In ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST (pp. 1-10).
14. Ozturk, T., Talo, M., Yildirim, E.A., Baloglu, U.B., Yildirim, O. and Acharya, U.R., 2020. Automated detection of COVID-19 cases using deep neural networks with X-ray images. Computers in Biology and Medicine, p.103792.
15. Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H., Albarqouni, S., Bakas, S., Galtier, M.N., Landman, B., Maier-Hein, K. and Ourselin, S., 2020. The future of digital health with federated learning. arXiv preprint arXiv:2003.08119.
16. https://www.zuehlke.com/en/insights/federated-learning-healthcare-ai- that-doesnt-risk-patient-data- privacy, extracted on 17/11/2020.