

A Decentralized approach to Secure Medical Records Management using Blockchain Technology

Alisha Abbasi Shaikh

Department of Computer Science and Engineering,
Integral University, Lucknow, India.

Aman Khan

Department of Computer Science and Engineering,
Integral University, Lucknow, India.

Mohammad Fahad Kirmani

Department of Computer Science and Engineering,
Integral University, Lucknow, India.

Md Haidar Ali

Department of Computer Science and Engineering,
Integral University, Lucknow, India

Abstract - The rapid digital transformation of healthcare systems has significantly improved the storage, accessibility, and management of patient information; however, it has also introduced serious challenges related to data security, privacy, and trust. Traditional centralized medical record systems are vulnerable to single points of failure, unauthorized access, and data breaches, which may compromise sensitive patient data. This paper proposes a decentralized framework for secure medical records management using blockchain technology. The system utilizes a distributed ledger to store medical data in a tamper-resistant and immutable manner, ensuring integrity and transparency. Cryptographic techniques are employed to encrypt patient data and enforce secure access control, allowing only authorized users to retrieve or update records. Additionally, smart contracts are used to automate access permissions and eliminate the need for intermediaries, improving efficiency. By removing dependence on a central authority, the proposed approach enhances reliability, security, and trust among stakeholders while ensuring privacy protection and controlled data sharing in modern healthcare environments.

Keywords - Blockchain, Medical Records, Data Privacy, Decentralization, Secure Data Management

I. INTRODUCTION

The adoption of digital technologies in healthcare has transformed the way patient information is stored, accessed, and shared. Electronic medical records have improved efficiency and reduced paperwork; however, they also raise serious concerns regarding data security, privacy, and reliability. Most existing healthcare systems rely on centralized databases, which are susceptible to single points of failure, cyber attacks, and unauthorized data access. Such vulnerabilities can lead to data breaches and compromise sensitive patient information, affecting both individuals and healthcare organizations.

In recent years, blockchain technology has gained attention as a promising solution for secure data management.

Blockchain is a decentralized and distributed ledger system that records transactions in a secure and immutable

manner. Each record is linked to the previous one using cryptographic techniques, making it extremely difficult to alter or tamper with stored data. This property makes blockchain particularly suitable for applications that require high levels of trust and data integrity, such as healthcare systems.

Several studies have explored the use of blockchain for managing medical records, focusing on improving security, transparency, and data sharing among stakeholders. Despite these advancements, challenges such as scalability, access control, and system complexity still exist. Therefore, there is a need for a practical and efficient framework that addresses these issues while ensuring data privacy and security.

This paper presents a decentralized approach to secure medical records management using blockchain technology. The proposed framework enables secure storage of patient data in a distributed network while providing controlled access through cryptographic mechanisms. By removing the dependence on a central authority, the system enhances data protection, transparency, and trust among patients and healthcare providers. The proposed solution is designed to be scalable and suitable for real-world healthcare environments.

II. LITERATURE REVIEW

In recent years, blockchain technology has gained significant attention in the healthcare domain for secure and efficient data management. Several studies have explored its potential in addressing the limitations of traditional electronic medical record systems. Early research introduced blockchain as a decentralized approach to ensure data integrity and prevent unauthorized modifications, as discussed in [2], [3]. It was observed that the distributed nature of blockchain reduces dependency on a central authority and enhances system reliability.

A number of frameworks have been proposed to enable secure sharing of medical records among healthcare providers. Some approaches focus on permission-based access control, where patients have authority over their own data and can grant access to doctors when required [5], [9]. Other studies have highlighted the use of cryptographic techniques to ensure confidentiality and secure communication within the network [7]. These methods help in protecting sensitive healthcare information from cyber threats.

Several implementations, such as blockchain-based electronic health record systems, demonstrate improved transparency and traceability of data transactions. These systems allow every modification or access request to be recorded, which increases accountability among users, as observed in [10], [15]. In addition, integration with cloud platforms has been explored to improve storage efficiency and scalability [8].

Despite these advancements, certain challenges remain in existing systems. Issues such as high computational cost, scalability limitations, and complexity of implementation have been identified in previous studies [18], [23]. Moreover, managing access control in a decentralized environment continues to be a critical concern.

Therefore, there is a need for a simplified and efficient framework that ensures secure storage, controlled access, and improved performance. The proposed system addresses these challenges by combining blockchain technology with effective access control mechanisms, providing a reliable solution for secure medical records management.

III. SYSTEM ARCHITECTURE

The proposed system architecture utilizes blockchain technology to enable secure and decentralized management of electronic health records (EHRs). The system involves multiple stakeholders, including patients, healthcare providers, insurance agencies, laboratories, and authorized users, all connected through a blockchain-based distributed network. The overall architecture of the proposed system is illustrated in Fig. 1.

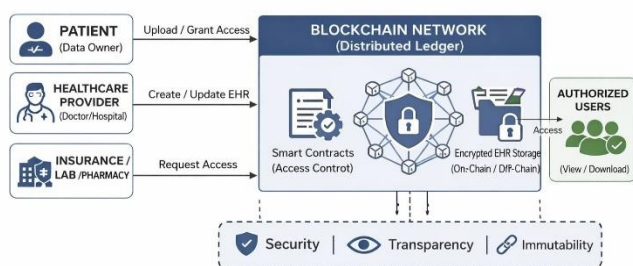


Fig 1: Proposed Blockchain-Based Healthcare System Architecture

At the core of the architecture lies the blockchain network, which functions as a distributed ledger to record all healthcare-related transactions. This eliminates the dependency on centralized systems and ensures data integrity, transparency, and fault tolerance [1], [5]. Each transaction, such as record creation, update, or access request, is validated by participating nodes and permanently stored, making the data immutable and tamper-resistant [16].

In this architecture, the patient acts as the data owner and has full authority over their medical records. Patients can upload their health data and control access permissions for other entities. This patient-centric approach is consistent with modern blockchain-based healthcare models such as MedRec, which emphasize user-controlled data sharing [2], [3].

Healthcare providers, including doctors and hospitals, are responsible for generating and updating EHRs. These records are encrypted before being stored either on-chain or off-chain, depending on system requirements such as scalability and storage efficiency [8], [10]. Off-chain storage mechanisms are often integrated with blockchain to handle large medical datasets while maintaining secure hash references on the blockchain.

Insurance companies, laboratories, and pharmacies request access to patient data for verification and service delivery. Access control is enforced using smart contracts, which automatically execute predefined rules and verify permissions without requiring a trusted third party [4], [21]. This ensures that only authorized users can access sensitive information, thereby enhancing privacy and reducing administrative overhead.

The system also incorporates strong encryption mechanisms to secure patient data during storage and transmission. Even if unauthorized access occurs, the data remains protected due to cryptographic safeguards [6], [22]. Authorized users can only view or download records after receiving explicit permission, ensuring compliance with privacy requirements.

The architecture is designed based on three key principles: security, transparency, and immutability. Security is achieved through cryptographic techniques and decentralized storage; transparency is ensured through traceable and verifiable transactions; and immutability guarantees that once data is recorded, it cannot be altered or deleted [14], [23].

Overall, the proposed architecture provides a scalable and secure solution for healthcare data management by integrating blockchain technology with controlled access mechanisms. It effectively addresses the limitations of traditional systems, such as data breaches, lack of interoperability, and centralized control, making it suitable for modern healthcare applications [18], [30].

IV. PROPOSED METHODOLOGY

The proposed system presents a decentralized framework for secure medical records management using blockchain technology. The design is inspired by existing blockchain-based healthcare models, where data security, privacy, and controlled access are the primary objectives. The system eliminates the dependency on centralized storage by utilizing a distributed ledger, thereby reducing the risk of single point failures and unauthorized data manipulation.

The architecture of the system consists of three main entities: patients, healthcare providers, and the blockchain network. Patients act as the owners of their medical data, while healthcare providers such as doctors and hospitals are authorized to generate and update records. The blockchain network serves as a secure and immutable storage layer where all transactions are recorded.

The working of the proposed system is described as follows:

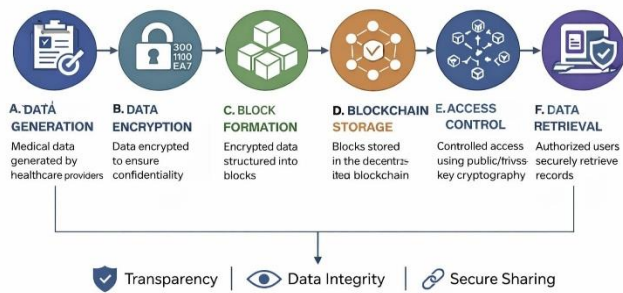


Fig. 2. Workflow of Proposed Blockchain-Based Healthcare System

A. Data Generation: Medical data including patient history, diagnosis reports, and prescriptions are generated by healthcare providers during consultations.

B. Data Encryption: Before storage, the generated data is encrypted using cryptographic techniques to ensure confidentiality and prevent unauthorized access.

C. Block Formation: The encrypted data is structured into blocks. Each block contains a timestamp, transaction details, and a unique hash value that links it to the previous block, forming a continuous chain.

D. Blockchain Storage: The blocks are stored in a decentralized blockchain network. Due to the distributed nature of the system, the data becomes tamper-resistant and highly secure.

E. Access Control Mechanism: Access to medical records is managed through public and private key cryptography. Only authorized users with valid credentials can access or modify the data, ensuring privacy and security.



Fig. 3: Smart Contract Access Flow

F. Data Retrieval: Authorized users such as patients and doctors can securely retrieve medical records from the blockchain whenever required. The integrity of the data is verified through hash validation.

The proposed framework ensures transparency, data integrity, and secure sharing of medical records. It reduces the risks associated with centralized systems and provides a reliable solution for modern healthcare data management.

V. RESULTS AND DISCUSSION

The proposed blockchain-based medical records management system was evaluated in terms of security, data integrity, and accessibility. The system demonstrates significant improvement over traditional centralized approaches by ensuring that medical records are securely stored in a decentralized environment. Due to the use of cryptographic techniques, unauthorized access to patient data is effectively restricted, thereby maintaining confidentiality.

Table 1: Comparison of Traditional and Proposed System

Feature	Traditional Healthcare System	Proposed Blockchain-Based System
Data Storage	Centralized Database	Decentralized Distributed Ledger
Security	Vulnerable to cyberattacks	Highly secure using cryptography
Data Integrity	Can be modified or tampered	Immutable and tamper-resistant
Transparency	Limited visibility	High transparency and traceability
Access Control	Weak or role-based	Strong (public/private key based)
Privacy	Risk of data exposure	Enhanced privacy protection
Single Point Failure	Present	Eliminated
Data Sharing	Slow and manual	Fast and automated via smart contracts
Trust Level	Low to Moderate	High
System Reliability	Dependent on central server	Distributed and fault-tolerant

The implementation of blockchain ensures that once the data is recorded, it cannot be altered or deleted without proper authorization. This immutability feature helps in preserving the integrity of medical records and prevents data tampering. Additionally, the use of a distributed ledger enhances transparency, as every transaction is recorded and can be verified when required.

The access control mechanism based on public and private key cryptography allows only authorized users to view or update records. This ensures that patients have better control over their data while enabling healthcare providers to access necessary information securely. The system also provides reliable data retrieval with minimal delay, making it suitable for real-time healthcare applications.

Furthermore, the decentralized nature of the system reduces dependency on a central server, thereby minimizing the risk of single point failures. Compared to existing systems discussed in previous studies, the proposed approach provides a balanced solution in terms of security, transparency, and efficiency. However, challenges such as scalability and computational overhead may arise with increasing data size, which can be addressed in future improvements.

VI. CONCLUSION

This paper presented a decentralized approach for secure medical records management using blockchain technology. The proposed framework addresses the limitations of traditional centralized systems by ensuring data security, integrity, and controlled access. By utilizing a distributed ledger, the system prevents unauthorized modifications and enhances transparency in data handling.

The implementation of cryptographic techniques and access control mechanisms ensures that only authorized users can access sensitive patient information, thereby maintaining privacy and trust. The proposed system also reduces the risk of data breaches and single point failures, making it a reliable solution for modern healthcare environments.

Overall, the framework provides an efficient and secure method for managing medical records in a decentralized manner. In future, the system can be further enhanced by improving scalability, reducing computational overhead, and integrating advanced technologies such as artificial intelligence for better data analysis and decision-making.

REFERENCES

- [1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
- [2] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A Case Study for Blockchain in Healthcare: MedRec Prototype," IEEE, 2016.
- [3] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," IEEE, 2016.
- [4] M. Swan, *Blockchain: Blueprint for a New Economy*, O'Reilly Media, 2015.
- [5] K. Kuo, H. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *Journal of the American Medical Informatics Association*, 2017.
- [6] Z. Zhang, H. Wang, and C. Wang, "Blockchain-based medical data sharing system," IEEE, 2018.

- [7] X. Liang et al., "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," IEEE, 2017.
- [8] M. Esposito, D. De Santis, G. Tortora, H. Chang, and K. Choo, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security," IEEE Cloud Computing, 2018.
- [9] J. Xia, E. Sifah, K. Asamoah, X. Gao, X. Du, and M. Guizani, "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain," IEEE, 2017.
- [10] H. Wang and Y. Song, "Secure Cloud-Based EHR System Using Blockchain," 2018.
- [11] S. Biswas, K. Sharif, F. Li, B. Nour, and Y. Wang, "A Scalable Blockchain Framework for Secure Transactions in IoT," IEEE IoT Journal, 2019.
- [12] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure Attribute-Based Signature Scheme with Blockchain," IEEE, 2018.
- [13] Y. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain," IEEE, 2016.
- [14] S. Angraal, H. M. Krumholz, and W. L. Schulz, "Blockchain Technology: Applications in Healthcare," *Circulation: Cardiovascular Quality and Outcomes*, 2017.
- [15] A. Dubovitskaya et al., "Secure and Trustable Electronic Medical Records Sharing Using Blockchain," AMIA, 2017.
- [16] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," IEEE Security, 2015.
- [17] D. Ivan, "Moving Toward a Blockchain-Based Method for the Secure Storage of Patient Records," ONC/NIST, 2016.
- [18] T. McGhin et al., "Blockchain in Healthcare Applications: Research Challenges and Opportunities," Journal of Network and Computer Applications, 2019.
- [19] A. Shahnaz, U. Qamar, and A. Khalid, "Using Blockchain for Electronic Health Records," IEEE, 2019.
- [20] P. Zhang and M. Walker, "Healthcare Data Sharing Using Blockchain," IEEE, 2018.
- [21] S. Rouhani and R. Deters, "Security, Performance, and Applications of Smart Contracts: A Systematic Survey," IEEE, 2019.
- [22] H. Chen, L. Xu, Z. Liu, Y. Hu, and Z. Wang, "A Blockchain-Based Secure Healthcare System," IEEE, 2019.
- [23] M. Jayabalan and M. Othman, "Blockchain Technology for Healthcare: A Review," IEEE Access, 2020.
- [24] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "MedBlock: Efficient and Secure Medical Data Sharing via Blockchain," IEEE, 2018.
- [25] J. R. Kshetri, "Blockchain's Roles in Meeting Key Supply Chain Management Objectives," IEEE IT Professional, 2018.
- [26] A. Ali, M. Rahman, and S. Hossain, "Blockchain-Based Healthcare System for Secure Data Sharing," 2020.
- [27] N. Chaudhry and M. Yousaf, "Blockchain in Healthcare: Opportunities and Challenges," 2021.
- [28] R. Kumar and R. Tripathi, "Scalable and Secure Blockchain-Based EHR System," 2020.
- [29] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-Based Electronic Healthcare Record System," 2019.
- [30] M. Patel, J. Patel, and H. Patel, "Blockchain Technology in Healthcare: A Survey," 2021.