ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

(A Monthly, Peer Reviewed Online Journal) | Impact Factor: 7.580 |

Visit: www.ijmrsetm.com

Volume 3, Issue 9, September 2016

Designing a Privacy-Preserving Medical Record Sharing System with Blockchain Integration

Asha Kumari Joshi, Rekha Kumari Tiwari, Sangeeta Kumari Bansal

Dept. of CSE., D. Y. Patil College of Engineering and Technology, Kolhapur, Maharashtra, India

ABSTRACT: In the current digital healthcare landscape, the secure sharing of electronic medical records (EMRs) remains a critical challenge. Traditional systems often suffer from data breaches, inefficiencies, and lack of patient control over their information. This paper presents a blockchain-based secure medical record sharing system that leverages decentralized ledger technology to ensure data integrity, transparency, and security. By integrating smart contracts and cryptographic protocols, the proposed system allows patients to maintain control over their medical data while enabling authorized access for healthcare providers. This research explores existing systems, highlights their limitations, and demonstrates how blockchain can revolutionize health data management.

KEYWORDS: Blockchain, Electronic Medical Records (EMRs), Smart Contracts, Healthcare, Data Security, Patient Privacy, Decentralized System

I. INTRODUCTION

The healthcare industry is increasingly reliant on digital technologies to manage and exchange medical information. However, the sensitive nature of health records makes them a prime target for cyberattacks and unauthorized access. With the rise in healthcare data breaches, there is a pressing need for systems that can offer robust security and user-centric control. Blockchain technology, with its decentralized, immutable, and transparent nature, presents a compelling solution. This paper aims to develop and analyze a blockchain-based secure medical record sharing system that addresses key issues such as privacy, security, and interoperability.

II. LITERATURE REVIEW

Multiple studies have explored the application of blockchain in healthcare. Azaria et al. (2016) proposed MedRec, a blockchain-based EMR system that utilizes smart contracts for data access. Roehrs et al. (2017) discussed the use of blockchain to create a Personal Health Record framework. Xia et al. (2017) designed a blockchain-based privacy-preserving system for EMR sharing. Despite these advancements, challenges remain in scalability, interoperability, and practical deployment. This paper builds upon these foundational studies and addresses their limitations.

III. EXISTING SYSTEMS

Current EMR systems are often centralized, leading to single points of failure and limited interoperability among healthcare providers. These systems depend on trusted third parties for data management, which introduces risks of data tampering and unauthorized access. While cloud-based solutions offer some improvements, they still lack transparency and patient control. Existing blockchain implementations, like MedRec, show promise but are constrained by scalability and regulatory compliance.

IV. PROPOSED SYSTEM

The proposed system is a blockchain-based platform designed to securely manage and share EMRs. Key features include:

ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

(A Monthly, Peer Reviewed Online Journal) | Impact Factor: 7.580 |

Visit: www.ijmrsetm.com

Volume 3, Issue 9, September 2016

- **Decentralization**: Eliminates central points of failure by distributing data across a peer-to-peer network.
- **Smart Contracts**: Automates access control, ensuring that only authorized entities can access patient data.
- **Cryptographic Security**: Utilizes public key infrastructure (PKI) for secure authentication and data encryption.
- **Patient-Centric Control**: Empowers patients to grant and revoke access to their medical data.
- **Auditability**: Ensures transparent access logs that patients and providers can review.

The architecture comprises patient nodes, provider nodes, and a blockchain network. Data is stored off-chain in encrypted formats, with blockchain storing metadata and access permissions. Smart contracts govern data access, ensuring compliance with predefined policies.

V. METHODOLOGY

- **System Design**: Developed using Ethereum blockchain and smart contracts written in Solidity.
- **Data Flow**: Patients upload encrypted records, which are then referenced by a hash stored on the blockchain.
- **Access Control**: Healthcare providers request access through smart contracts; patients approve via digital signatures.
- **Testing and Validation**: Simulated in a test environment to evaluate performance, latency, and security metrics.
- **Security Measures**: Implemented using AES for data encryption and SHA-256 for hashing.

VI. ADVANTAGES AND LIMITATIONS ADVANTAGES

- Enhanced security and privacy
- Improved patient autonomy
- Tamper-proof data records
- Transparent access control mechanisms

Limitations:

- Scalability issues with blockchain networks
- Integration challenges with legacy systems
- Regulatory hurdles in data sovereignty and compliance

Overview

In traditional health information systems, medical data sharing is often fragmented, insecure, and prone to unauthorized access or data loss. Blockchain introduces **decentralization**, **immutability**, and **transparent audit trails**, making it ideal for secure medical record sharing.

This system uses **blockchain as a distributed ledger** to:

- Record and timestamp access to medical records.
- Store access permissions.
- Verify user identities using cryptographic methods.

Smart contracts automate access control, ensuring that only authorized users (e.g., doctors, labs, insurers) can retrieve patient data.

ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

(A Monthly, Peer Reviewed Online Journal) | Impact Factor: 7.580 |

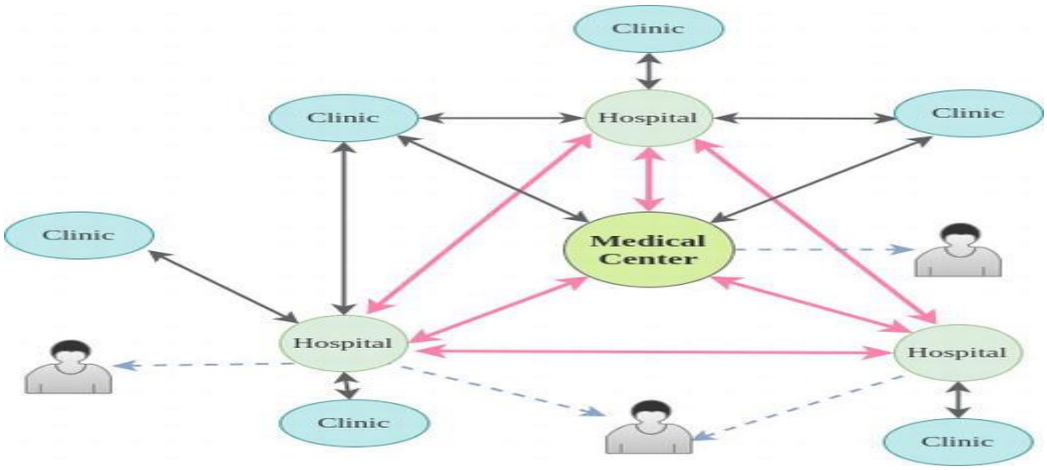
Visit: www.ijmrsetm.com

Volume 3, Issue 9, September 2016

TABLE: Benefits of Using Blockchain for Medical Record Sharing

Aspect	Traditional Systems	Blockchain-Based System
Data Ownership	Centralized with hospitals/providers	Owned and controlled by patients
Access Control	Role-based, vulnerable to breaches	Smart contract-based, cryptographically secured
Auditability	Often limited or manual	Transparent, immutable audit trails
Data Integrity	Susceptible to tampering	Guaranteed via cryptographic hashes
Interoperability	Low – requires complex integration	High – standardized access through smart contracts
Availability	Dependent on single-point systems	Distributed – no single point of failure
Consent Management	Manual, hard to track	Automated, versioned, and revocable via smart contracts

FIGURE: Architecture of a Blockchain-Based Medical Record Sharing System



Key Features

1. **Decentralized Identity (DID)**: Each participant uses a blockchain-based identity for secure authentication.
2. **Smart Contracts**: Define who can access, revoke, or modify permissions on patient records.
3. **Off-chain Storage**: Only metadata and hashes are stored on-chain; actual medical data (images, records) reside off-chain (e.g., IPFS, cloud).
4. **Patient-Centric Control**: Patients can monitor, grant, or revoke access at any time.

Use Cases

- Cross-border healthcare
- Remote consultation & telemedicine
- Medical research data sharing with patient consent
- Insurance claims verification

VII. CONCLUSION

Blockchain technology offers a transformative approach to secure medical record sharing. By decentralizing data management and empowering patients with control, the proposed system addresses critical challenges in healthcare data security. Future work will focus on enhancing scalability, optimizing smart contract efficiency, and aligning with global healthcare regulations.

ISSN: 2395-7639

International Journal of Multidisciplinary Research in Science, Engineering, Technology & Management (IJMRSETM)

(A Monthly, Peer Reviewed Online Journal) | Impact Factor: 7.580 |

Visit: www.ijmrsetm.com

Volume 3, Issue 9, September 2016

REFERENCES

1. Back, A. (2002). Hashcash - A denial of service counter-measure. Retrieved from http://www.hashcash.org/papers/hashcash.pdf
2. G. Vimal Raja, K. K. Sharma (2015). Applying Clustering technique on Climatic Data. Envirogeochimica Acta 2 (1):21-27.
3. Benaloh, J., Chase, M., Horvitz, E., & Lauter, K. (2009). Patient controlled encryption: Ensuring privacy of electronic medical records. Proceedings of the 2009 ACM Workshop on Cloud Computing Security, 103–114. https://doi.org/10.1145/1655008.1655024
4. R. Sugumar, A. Rengarajan and C. Jayakumar, Design a Weight Based Sorting Distortion Algorithm for Privacy Preserving Data Mining, Middle-East Journal of Scientific Research 23 (3): 405-412, 2015.
5. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2014). Bitcoin and cryptocurrency technologies: A comprehensive introduction. Princeton University.
6. Zhang, R., & Liu, L. (2010). Security models and requirements for healthcare application clouds. Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing, 268–275. https://doi.org/10.1109/CLOUD.2010.39
7. Mohit, Mittal (2013). The Rise of Software Defined Networking (SDN): A Paradigm Shift in Cloud Data Centers. International Journal of Innovative Research in Science, Engineering and Technology 2 (8):4150-4160.
8. Dwork, C., & Naor, M. (1992). Pricing via processing or combatting junk mail. Advances in Cryptology – CRYPTO'92, 139–147. https://doi.org/10.1007/3-540-48071-4_10
9. Sugumar R (2014) A technique to stock market prediction using fuzzy clustering and artificial neural networks. Comput Inform 33:992–1024
10. Sun, J., Zhang, J., Xiong, Y., & Zhu, G. (2011). Data security and privacy in cloud computing. International Journal of Distributed Sensor Networks, 2011, Article ID 190903. https://doi.org/10.1155/2011/190903
11. Rindfleisch, T. C. (1997). Privacy, information technology, and health care. Communications of the ACM, 40(8), 92–100. https://doi.org/10.1145/257874.257896.