HEALTHLOCK: BLOCKCHAIN-BASED SECURE HEALTHCARE DATA MANAGEMENT SYSTEM

Neetansh Bhowad

Student, MSc. Information and Cybersecurity
Department of Information Technology
Guru Nanak Khalsa College, Mumbai, India

Abstract

The rapid digital transformation of healthcare systems has led to an exponential increase in the generation and exchange of sensitive medical data. However, traditional centralized healthcare infrastructures are highly vulnerable to cyber threats, unauthorized access, and data manipulation. These limitations significantly affect patient privacy, trust, and system efficiency. This research presents **Health Lock**, a blockchain-based decentralized healthcare data management system that ensures secure, transparent, and tamper-proof handling of medical records. The system integrates blockchain technology with smart contracts and Interplanetary File System (IPFS) to provide a hybrid storage mechanism that enhances scalability and reduces operational costs. Unlike traditional systems, Health Lock introduces a patient-centric model where individuals maintain full ownership of their medical data and control access permissions. The implementation demonstrates improved data integrity, transparency, and security through cryptographic hashing, role-based access control, and decentralized storage.

Keywords: Blockchain, Healthcare, IPFS, Smart Contracts, Data Security, Patient Privacy.

1. INTRODUCTION

Healthcare systems today handle vast amounts of sensitive patient data, including medical history, diagnostic reports, and treatment records. With the increasing adoption of Electronic Health Records (EHRs), the need for secure and efficient data management has become more critical than ever. Traditional systems rely on centralized databases, which introduce several risks:

- **Single point of failure:** If the central server goes down, the entire system is inaccessible.

- **High susceptibility to cyberattacks:** Centralized hubs are primary targets for ransomware and data breaches.
- **Unauthorized data access:** Lack of granular control over who views sensitive records.
- **Data inconsistency:** Information is often fragmented across different platforms.

Health Lock addresses these challenges by leveraging blockchain technology to create a decentralized, secure, and transparent healthcare ecosystem where data is immutable and access is strictly controlled.

2. RESEARCH CONTRIBUTION

This research introduces a comprehensive blockchain-based framework with the following contributions:

- A decentralized architecture eliminating reliance on centralized servers.
- Smart contract-based access control for secure data interaction.
- Integration of **IPFS with Pinata** for scalable storage of large medical files (e.g., MRI, X-rays).
- Implementation of patient-controlled data ownership models.
- A transparent and auditable system for tracking all medical data transactions.

3. SYSTEM DESIGN AND ARCHITECTURE

The proposed Health Lock system follows a multi-layered architecture consisting of:

3.1 Blockchain Layer

The blockchain serves as the ledger for transaction records rather than full files. This layer maintains immutable logs of all medical data operations and uses cryptographic hashing to ensure that the data recorded cannot be altered retroactively.

3.2 Smart Contract Layer (Core Logic)

Implemented using **Solidity**, smart contracts act as the backbone of the system, governing:

- **User Authentication:** Secure login and identity verification.
- **Role-Based Access Control (RBAC):** Utilizing modifiers like onlyDoctor and onlyPatient to restrict data modification and viewing rights.

- **Doctor Verification:** An admin-controlled registration process ensures only validated medical professionals can enter the network.

3.3 IPFS Storage Layer (Pinata Integration)

To overcome the high costs and scalability limitations of on-chain storage, HealthLock utilizes a **Hybrid Storage** model:

1. **Storage:** Large files are stored on IPFS via Pinata.
2. **Referencing:** IPFS generates a unique Content Identifier (CID).
3. **Linking:** Only the CID is stored in the smart contract on the blockchain.

This ensures the system is tamper-proof (any change to a file generates a new CID) while remaining highly scalable and cost-effective.

3.4 Security Mechanisms

- **Encryption:** Files are encrypted before being uploaded to IPFS.
- **RBAC:** CIDs are only accessible to authorized users.
- **Auditability:** Every transaction is recorded, providing a complete history for forensic investigation.

4. SYSTEM WORKFLOW

1. **Registration:** The patient registers; doctors request access and are verified by an admin.
2. **Upload:** A verified doctor uploads a record; it is sent to IPFS and a CID is generated.
3. **Permission:** The CID is recorded in a smart contract. The patient grants access to specific doctors.
4. **Retrieval:** Authorized users use the CID to retrieve the original encrypted file from IPFS.
5. **Audit:** Every step is time-stamped and logged on the blockchain.

5. IMPLEMENTATION DETAILS

The system was developed using a modern decentralized tech stack:

- **Solidity:** For backend smart contract logic.
- **IPFS (Pinata):** For decentralized file storage.

- **Web UI:** Three distinct dashboards for Patients (view/grant access), Doctors (upload/update), and Admins (user management).

6. RESULTS AND DISCUSSION

Health Lock demonstrates a significant reduction in risks associated with centralized data management. By decentralizing the storage and the authority over the data, the system effectively mitigates the threat of unauthorized modifications and data loss. The audit logs ensure that even if a dispute arises, a transparent record of all interactions is available.

7. TECHNICAL CHALLENGES

While effective, the implementation highlighted certain challenges:

- **Blockchain Scalability:** Managing transaction speeds on mainnets.
- **Latency:** Time taken for block confirmations.
- **Regulatory Compliance:** Aligning decentralized systems with existing laws like HIPAA and GDPR.

8. CONCLUSION

Health Lock provides a secure, decentralized, and scalable solution for healthcare data management. By combining blockchain with IPFS and smart contracts, the system ensures data integrity, privacy, and accessibility. This patient-centric model empowers individuals with full control over their records, offering a robust alternative to traditional healthcare infrastructures.

9. FUTURE SCOPE

Future developments will focus on:

- **AI Diagnostics:** Integrating machine learning for automated diagnosis based on vault data.
- **IoT Integration:** Real-time logging from wearable health devices.
- **Layer-2 Solutions:** Implementing sidechains to further reduce transaction latency.

10.REFERENCES

1. A. Bisht, A. K. Das, D. Niyato and Y. Park, ”Efficient Personal-Health-Records Sharing in Internet of Medical Things Using Searchable Symmetric Encryption, Blockchain, and IPFS,” in IEEE Open Journal of the Communications Society, vol. 4, pp. 2225-2244, 2023, doi: 10.1109/OJCOMS.2023.3316922.

2. Azaria, A., et al. ”MedRec: Using Blockchain for Medical Data Access and Permission Management,” IEEE Blockchain, 2016.

3. Zhang, P., et al. ”HealthChain: Blockchain for Healthcare Data Management,” IEEE Transactions on Blockchain, 2018.

4. Patel, V. ”A Blockchain-Based Approach for Secure Electronic Health Records,” 2020.

5. Jawalkar, S., Shende, R., Selokar, R., Sendre, S., & Vairagde, R. (2024, March). Carbon Credit Transfer System using Blockchain. In 2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Pro- cessing (INCOS) (pp. 1-6). IEEE.

6. Vairagade, R., Bitla, L., Judge, H. H., Dharpude, S. D., & Kekatpure, S. S. (2022, April). Proposal on nft minter for blockchain-based art-work trading system. In 2022 IEEE 11th International Conference on Communication Systems and Net- work Technologies (CSNT) (pp. 571-576). IEEE.

7. Bhandari, B., Vairagade, R., Trivedi, H., Thakre, H., Indurkar, G., & Yadav,A. (2023, April). Decentralized medical healthcare record management system using blockchain. In 2023 11th International Conference on Emerging Trends in Engineering & Technology-Signal and Information Processing (ICETET-SIP) (pp. 1-5). IEEE.