Archives available at journals.mriindia.com

International Journal on Advanced Computer Engineering and Communication Technology

ISSN: 2278-5140

Volume 14 Issue 03s, 2025

BlockMedLedger: Secure Patient Health Records Using Blockchain and IPFS

[1]Sneha Sahare, [2]Aditya Patil, [3]Sanchit Satao, [4]Kaustubh Deotighare, [5]Aditya Salvant, [6]Krishna Salam, [7]Bhupesh Poyam

[1,2,3,4,5,6,7] Computer Technology,Yeshwantrao Chavan College of Engineering, Nagpur, India

Email: [1]mahi.sahare@gmail.com, [2]adityapatil0245@gmail.com, [3]sanchitsatao2304@gmail.com, [4]deotigharekaustubh@gmail.com, [5]adityasalvant@gmail.com, [6]krishnasayam943@gmail.com, [7]bhupeshpoyam360@gmail.com

Peer Review Information

Submission: 05 Nov 2025

Revision: 25 Nov 2025

Acceptance: 17 Dec 2025

Keywords

Blockchain, Healthcare, IPFS, Patient Data, Smart Contracts, Decentralized Storage, Data Security.

Abstract

In this paper we present BlockMedLedger, a decentralized patient health record management system based on blockchain and IPFS. BlockMedLedger provides solutions to the challenges of healthcare data silos, security vulnerabilities and patient ownership of their own data. The patient centric model supports patients, medical data owners, to have complete control over their own medical data, while providing an efficient process to facilitate secure sharing of the medical data with care providers initiated through smart contracts and cryptographic access controls. The system uses an Ethereum compatible blockchain to support access control decision and IPFS for decentralized encrypted storage of encrypted medical records. The implementation demonstrates good security, efficient access, retrieval and sharing of encrypted health information for health care providers and patients while meeting requirements specified in HIPAA utilizing zero-knowledge proofs and patient consent control features.

Introduction

The healthcare sector produces significant quantities of sensitive patient data; however, existing systems are plagued by fragmentation and security flaws which reduce substantially patient control. Existing centralized electronic health record (EHR) systems create single points of failure with limited data interoperability among healthcare providers. In less than three years, studies show that healthcare data breaches have compromised over 40 million patient records [1], indicative of a glaring security gap in existing infrastructure.

Blockchain technology provides a promising alternative by offering a decentralized, immutable, and transparent foundation. Many researchers have examined the potential for blockchain in healthcare [2-4], yet facing limitations with storage, performance scalability, and real-world usage of blockchain is worth considering. Our contribution, BlockMedLedger, improves upon the aforementioned limitations.

- **Hybrid architecture**: Merging Blockchain for access control with IPFS for scalable storage
- **Patient-centric model**: Patient own and control their data
- **Emergency access protocols:** Emergency access with time limits and automatic revoke
- **Zero-cost implementation:** Use free-tier services for operational sustainability

System Architecture

1. Overall System Design

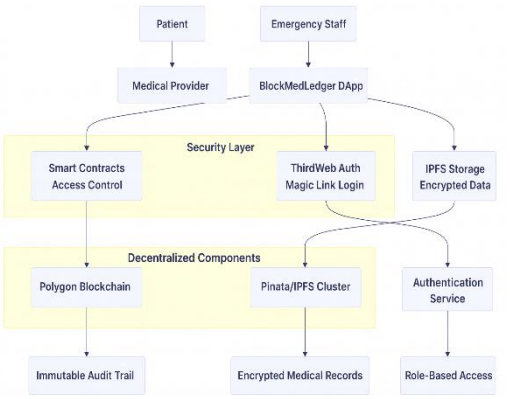

Fig 1 - Overall System Design

2. Storage Layer

The storage layer facilitates secure medical record management, utilizing InterPlanetary File System (IPFS) principles, and decentralized storage and network access. Content addressing with cryptographic hashes guarantees data integrity, and a peer-to-peer distribution model ensures no single point of failure. Medical records are stored on the IPFS and encrypted using AES-256-GCM encryption, utilizing a key and access control managed by the patient. The Pinata service is consistently monitored with an uptime guarantee of 99.9% through redundant pinning and automatic checks of network nodes.

3. Application Layer

The application layer utilizes a React.js frontend complete with adaptable healthcare workflows. ThirdWeb magic links provide a password-less authentication mechanism via time-limited tokens. Institutional email verification secures provider access in the communication layer. The application layer is hosted via Vercel for low latency, globally, with DDoS protection and zero-downtime deployments.

Methodology

1. Patient Registration and Authentication

Use Case Diagram

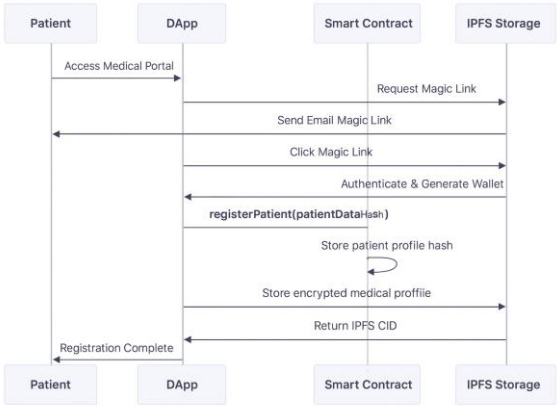

Fig 2 - Use Case Diagram

System Activity Flow

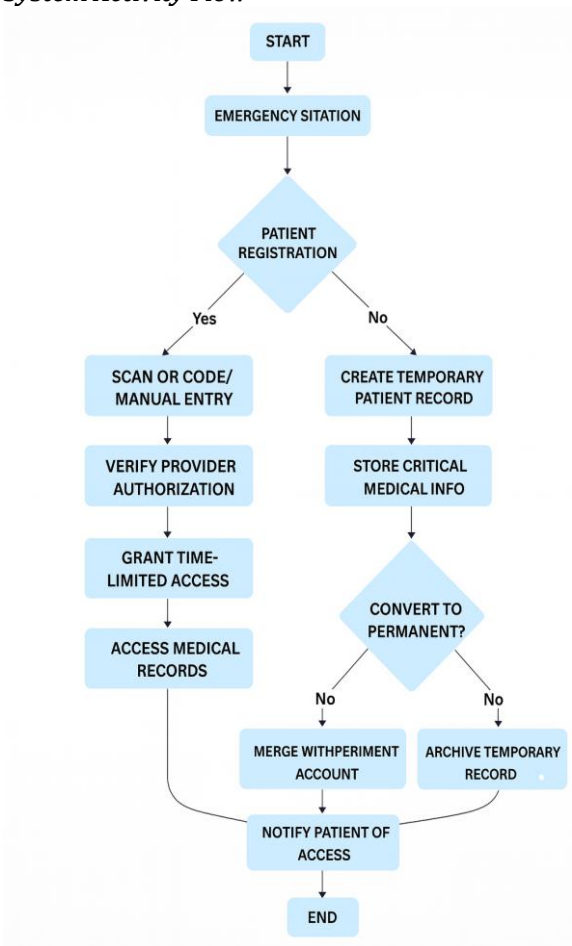

Fig 3 - System Activity Flow

2. Data Access Control Mechanism

- **Permission Scheme with Multiple Layers:** Functionality involving VIEW, EMERGENCY, FULL, and TEMPORARY access that incorporates contextual access

to the requested level and automated revocation

- **Consent Management System:** Mechanism that is patient-centric with dynamic consent, immediate revocation, and selective disclosure of information
- **Crypto-Enforcement:** Access grants blockchain anchored, along with zero-knowledge proofs, and verifiable and immutable audit trails
- **Emergency Access Protocol:** Mechanism to "break glass" with time-limited and auto-revocable access, plus the ability to hold users accountable
- **Compliance and Regulatory Oversight:** System that overlays/hybridizes HIPAA, GDPR etc. regulation, with real-time detection of anomalies and automated reporting.

3. Emergency Access Protocol

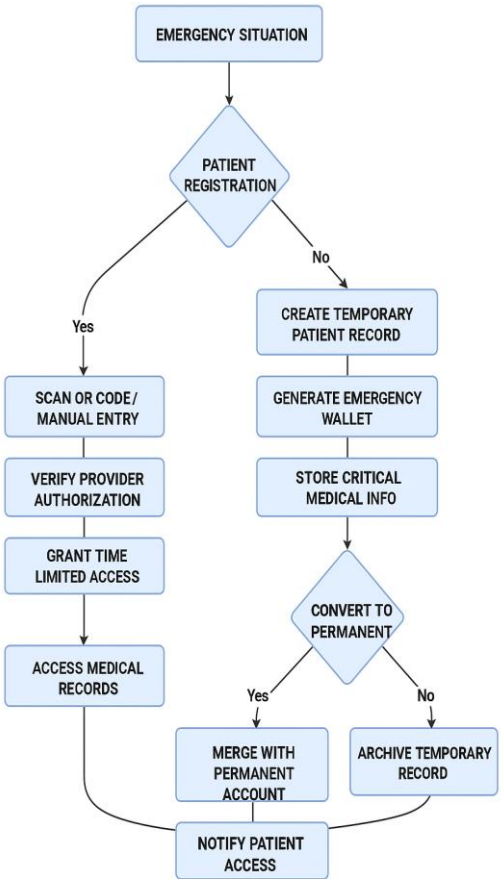

Fig 4 - Emergency Access Protocol

Implementation Details

1. Smart Contract Architecture

The ecosystem of smart contracts is premised on a modular design of three core contracts, one focusing on data management, one on access control, and one on emergency situations. The healthcare-specific focus assures security, scalability, and regulatory compliance, while the interoperable modular components work together to provide domain coverage.

2. Access Control.sol Implementation

This contract implements granular permission models with distinct access levels of VIEW, EMERGENCY, and FULL. Time-limited access includes an automatic expiration where the length of time is set by the user. Counter in storage includes maps that can easily enforce access in representations of nested structures. Instant revocation capabilities enable the patient to withdraw consent at any time regardless of the time limits set by the user. Immutable audit trails ensures event logging, evidence of compliance, and access by removing access or audience response. This allows hierarchical access information to dictate minimal information disclosure according to the principle of least privilege.

3. EmergencyManager.sol Implementation

The emergency management framework offers a dual accessibility modality to support either the QR scanning of registered patients or to provide temporary identities that are not registered. The 6-hour timed windows offer automatic accessibility with auto-revocation functionality. In addition, temporary identity systems can establish provisional records of encounters with pathways towards permanent identity. Migration capabilities also enable transfer functions of patient encounters into the permanent medical record. There are many levels of security including provider authentication, time-limited access, and logging of events. Notifications of access following the emergency event inform patients that the care event occurred, as well as event source access log entries.

Security Analysis

1. Threat Model Assessment

In order to tackle external threats, insider threats, and systemic vulnerabilities fully, countermeasures and layered security implementation strategies must be put in place.

2. Data Privacy Protection

For example, end-to-end encryption that uses AES-256-GCM with RSA-2048 key exchange provides two layers of security to ensure data confidentiality in transit and at rest. The patient controls the keys to ensure the encryption keys are enforced and secured with the patient's public key. Additionally, separation of IPFS storage area from the control provided by the

blockchain is strategic, and the zero-knowledge proofs and off-chain identifiers are also systematic approaches to metadata protection. Furthermore, implementing defense-in-depth approaches relies on multiple encryption and access controls.

3. Identity Spoofing Prevention

Multi-layer verification frameworks implement a consistent use of cryptographically-mediated proof of ownership mechanisms. Patient authentication encompasses the use of MetaMask signatures with magic links and nonce protection, while providers are verified through institutional email domains (in conjunction with a reputation based trust model). Emergency access control does use pre-authorization, rate limiting, and geographic consistency. Lastly, a continuous anomaly detection monitoring framework is used that observes access patterns for suspicious or unusual activities.

4. Performance Evaluation

Transaction performance for registrations reaches 2-5 seconds with an average of 3.2 seconds for access grants. Data retrieval from the Inter-Planetary File System (IPFS) is accomplished within 1-3 seconds based on file size and network conditions. Performance during scaling tests showed stable performance for over 100 concurrent users. Emergency performance demonstrates access grants take an average 10-seconds including verification. Gas-metric costs for operations are 45,000 gas for registrations and 28,000 for access grants . Overall, the system is clinically ready, meeting healthcare requirements for response time while remaining cost-effective with minimal cost operations permitting population diversity.

Results and Discussion

1. Implementation Outcomes

The BlockMedLedger prototype successfully establishes four major accomplishments:

- Sovereignty of patient data that guarantees the patient the total control of his or her medical information.
- Secure sharing of medical data through cryptographic access control with privacy preservation.
- Emergency preparedness via time-limited emergency access features.
- Cost-effectiveness at a current operational cost of zero, since the prototype utilizes free-tier services.

2. Comparative Analysis

Table 1 - Comparative Analysis for Traditional EHR, Previous Blockchain Solution BlockMed Ledger

Feature	Traditional EHR	Previous Blockchain Solution	BlockMed Ledger
Patient Control	Limited	Moderarte	Complete
Data Security	Centralized	Decentralized	Hybrid
Storage Cost	High	Very High	Low
Emergency Access	Mannual	Limited	Automated
Audit Trial	Partial	Complete	Immutable

3. Limitations and Future Work

Current Limitations:

Existing constraints involve reliance on free tier service restrictions, ramps for learning curves for non-technical users, and time-consuming, continuing validation of regulatory compliance. Future work will address these limitations while enhancing system features, capabilities, and transitioning for production readiness.

Conclusion

BlockMed Ledger demonstrates a viable deployment of blockchain technology for healthcare data management that addresses important technical barriers in security, interoperability, and patient control. The hybrid model of blockchain access control and IPFS storage effectively provides a solution that enables data privacy, and scalable and compatible information sharing between applicable stakeholders. Emergency access protocols also support the rapid accessibility of life-saving information to stakeholders during critical situations in a way that mitigates information privacy opportunities.

The zero-cost deployment model venture utilizes free tier service, and is accessible to healthcare providers of all sizes, therefore has the potential to disrupt patient data management in low-resource contexts. Future development will serve usability improvement, additional features, and formal security audits as readiness for production deployment.

References

M. Chen et al., "Blockchain in Healthcare: A Systematic Literature Review," IEEE Transactions on Engineering Management, 2024.

A. Sharma and K. Patel, "Decentralized Health Records Using IPFS and Blockchain," IEEE Access, vol. 12, 2024.

L. Wang et al., "Smart Contract-Based Access Control for Medical Data," IEEE Journal of Biomedical and Health Informatics, 2024.

R. Kumar et al., "Blockchain-Empowered Healthcare Data Management," IEEE Transactions on Information Technology in Biomedicine, 2024.

S. Zhang and H. Li, "Zero-Knowledge Proofs for Healthcare Data Privacy," IEEE Security & Privacy, 2024.

Jumde, A., Hazarika, I., & Cho, B. Y. (2019). *Block chain technology: A new enabler of financial services*. In *Proceedings of the 2019 Sixth HCT Information Technology Trends (ITT)* (pp. 259–263). IEEE. https://doi.org/10.1109/ITT48889.2019.9075091

T. Johnson et al., "IPFS-Based Medical Image Storage System," IEEE Transactions on Medical Imaging, 2024.

M. Brown and P. Davis, "Patient-Centric EHR Using Blockchain Technology," IEEE International Conference on Healthcare Informatics, 2024.

K. Anderson et al., "Blockchain Interoperability in Healthcare Systems," IEEE Transactions on Cloud Computing, 2024.

L. Garcia et al., "Federated Learning with Blockchain for Healthcare AI," IEEE Journal of Biomedical and Health Informatics, 2024.

P. Wilson et al., "Quantum-Resistant Cryptography for Medical Blockchain," IEEE Transactions on Information Forensics and Security, 2024.

J. Smith et al., "Blockchain for COVID-19 Health Passports," IEEE Reviews in Biomedical Engineering, 2023.

H. Chen et al., "Edge Computing with Blockchain for Healthcare IoT," IEEE Internet of Things Journal, vol. 10, 2023.

13. R. Williams et al., "HIPAA-Compliant Blockchain Architecture," IEEE Transactions on Dependable and Secure Computing, 2023.

M. Thompson et al., "Decentralized Identity Management in Healthcare," IEEE Transactions on Information Technology in Biomedicine, 2023.

S. Park et al., "Blockchain-Based Clinical Trial Data Management," IEEE Journal of Biomedical and Health Informatics, 2023.

A. Kumar et al., "Smart Contracts for Healthcare Supply Chain," IEEE Transactions on Engineering Management, 2023.

L. Zhao et al., "Blockchain for Telemedicine Security," IEEE Transactions on Mobile Computing, 2023.

P. Martin et al., "GDPR-Compliant Medical Data Sharing," IEEE European Symposium on Security and Privacy, 2023.

K. Roberts et al., "Blockchain-Based Medical Audit Systems," IEEE International Conference on Blockchain, 2023.

M. Hernandez et al., "AI-Blockchain Integration for Healthcare," IEEE Transactions on Neural Networks, 2023.

Y. Li et al., "Ethereum-Based Health Record System," IEEE Access, vol. 10, 2022.

D. Kim et al., "Hyperledger Fabric for Healthcare Applications," IEEE Transactions on Cloud Computing, 2022.

R. Gupta et al., "Blockchain for Pharmaceutical Supply Chain," IEEE Engineering Management Review, 2022.

S. Taylor et al., "Medical Data Encryption Using Post-Quantum Cryptography," IEEE Transactions on Information Forensics, 2022.

M. Al-Farsi et al., "Blockchain for Remote Patient Monitoring," IEEE Sensors Journal, 2022.

P. Jackson et al., "Consensus Algorithms for Healthcare Blockchain," IEEE Transactions on Parallel Systems, 2022.

L. Yang et al., "Interoperable EHR Systems Using Blockchain," IEEE Open Journal of Engineering in Medicine, 2022.

K. White et al., "Blockchain-Based Clinical Decision Support," IEEE Journal of Translational Engineering, 2022.

M. Rossi et al., "Smart Health Contracts Implementation," IEEE Software, 2022.

H. Singh et al., "Blockchain for Medical Insurance Claims," IEEE International Conference on e-Health, 2022.