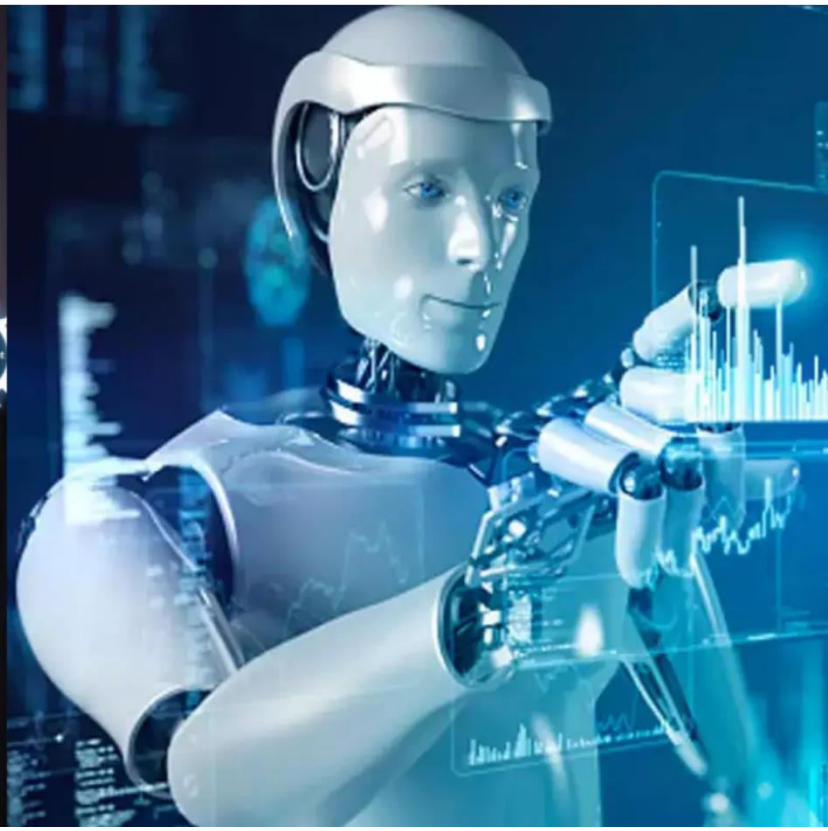
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 4, April 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504242|

A Blockchain-Based Framework for Secure Medical Record Management with Fine-Grained Access Control

S. Janaki[1], S.Nishanthini[2], C. Kayalvizhi [3], Mrs. P. Vennila[4]

B. Tech Student Final Year, Department of AI&DS, Sir Issac Newton College of Engineering and Technology, Pappakovil, Nagapatinam, Tamil Nadu, India[1]

B. Tech Student Final Year, Department of AI&DS, Sir Issac Newton College of Engineering and Technology, Pappakovil, Nagapatinam, Tamil Nadu, India [2]

B. Tech Student Final Year, Department of AI&DS, Sir Issac Newton College of Engineering and Technology, Pappakovil, Nagapatinam, Tamil Nadu, India[3]

Assistant Professor, Department of AI&DS, Sir Issac Newton College of Engineering and Technology, Pappakovil, Nagapatinam, Tamil Nadu, India[4]

ABSTRACT: The rapid digitization of healthcare systems has significantly improved medical data accessibility but has also introduced critical security and privacy challenges. Traditional Electronic Health Record (EHR) systems rely on centralized architectures, making them vulnerable to data breaches, unauthorized access, and single points of failure. This paper proposes a blockchain-based framework for secure medical record management with fine-grained access control. The system leverages a permissioned blockchain network and smart contracts to ensure data integrity, transparency, and controlled access. Attribute-based access control (ABAC) mechanisms are integrated to allow precise authorization based on user roles and attributes. The proposed model enhances patient data privacy, ensures tamper-proof storage, and provides complete auditability of access logs. Experimental results demonstrate improved security, transparency, and scalability compared to conventional systems.

KEYWORDS—Blockchain, electronic medical records, access control, attribute-based encryption, IPFS, healthcare security

I. INTRODUCTION

The widespread adoption of Electronic Health Records (EHRs) and Electronic Medical Records (EMRs) has transformed healthcare delivery, enabling real-time data access, coordinated treatment, and data-driven research . However, this digitization has also expanded the attack surface for cyber threats, with healthcare data breaches affecting millions of patients annually. Traditional Electronic Health Record (EHR) systems experience centralized vulnerabilities which explain how healthcare data breaches reach about 45% of cases .

Conventional access control mechanisms, such as Role-Based Access Control (RBAC), rely on centralized servers that present single points of failure and are susceptible to distributed denial-of-service (DDoS) attacks . Furthermore, patients often lack visibility and control over who accesses their sensitive medical information, creating significant privacy concerns. The Office of the National Coordinator (ONC) for Health Information Technology actively seeks patient-centric health information exchange ideas that can assist shift ownership of information from suppliers to patients

Blockchain technology has emerged as a promising solution to address these challenges . Its decentralized nature ensures data integrity and availability, eliminating reliance on a central authority. Key properties including immutability, transparency, and cryptographic security make blockchain particularly suitable for healthcare applications where data provenance and auditability are paramount . Smart contracts enable automated enforcement of

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504242|

access policies, while integration with decentralized storage systems addresses blockchain's inherent scalability limitations for large medical files.

1. Decoupled architecture: We propose a hybrid storage model that separates content storage from access control and audit, storing encrypted medical records off-chain while maintaining cryptographic commitments and access policies on-chain.
2. Fine-grained access control: We implement ciphertext-policy attribute-based encryption (CP-ABE) that enables patients to specify granular access rules based on recipient attributes, supporting selective disclosure of sensitive information.
3. Comprehensive auditability: The framework maintains immutable audit logs of all access events through smart contracts, enabling regulatory compliance and forensic analysis.

II. RELATED WORK

The application of blockchain technology to healthcare data management has received significant research attention in recent years. This section reviews representative approaches and identifies gaps addressed by our work.

MedRec was one of the pioneering blockchain-based systems for electronic medical records, utilizing Ethereum smart contracts to manage patient-provider relationships . While MedRec demonstrated the feasibility of blockchain for healthcare, it lacked fine-grained access control mechanisms and suffered from the scalability limitations of public blockchain storage

MedShare proposed a decentralized framework for secure EHR sharing using attribute-based encryption . The system enables multi-keyword boolean search operations over encrypted EHRs and embeds access policies in search results on the blockchain. However, MedShare's implementation relies on centralized components that reintroduce single points of failure.

The DPEM (Decentralized EMR Management) structure introduced a four-layer architecture encompassing data preparation, exchange, storage, and access control . DPEM employs elliptic curve-based content extraction signatures (EC-CES) that allow patients to filter sensitive data during sharing, preventing privacy leakage. Additionally, ciphertext-policy attribute-based encryption enables data owners to protect cloud storage while granting authorized access.

ACHealthChain leverages Hyperledger Fabric to implement a dedicated PolicyChain for fine-grained access control and revocation . The framework structures patient healthcare data into separate subchains for EHRs and diagnoses with permissioned access, while LogChain enhances auditing and accountability. Experimental results demonstrate throughput improvements of 19.7% and latency reductions of 87% compared to existing frameworks.

MedBioCh integrates biometric authentication with blockchain technology, utilizing Gabor filters and chaotic systems for revocable biometric feature extraction . The system employs IPFS for decentralized storage and addresses the critical limitation of traditional biometrics where compromised features cannot be changed.

HealthGuard combines Ethereum with MetaMask for authentication and decentralized storage solutions, demonstrating reduced healthcare administration costs through smart contracts and decentralized applications . The framework emphasizes patient control over healthcare records with built-in privacy features.

Despite these advances, existing systems exhibit limitations including incomplete access control granularity, insufficient attention to regulatory compliance, and lack of comprehensive performance evaluation. Our work addresses these gaps by integrating CP-ABE with permissioned blockchain technology while explicitly addressing HIPAA and GDPR requirements.

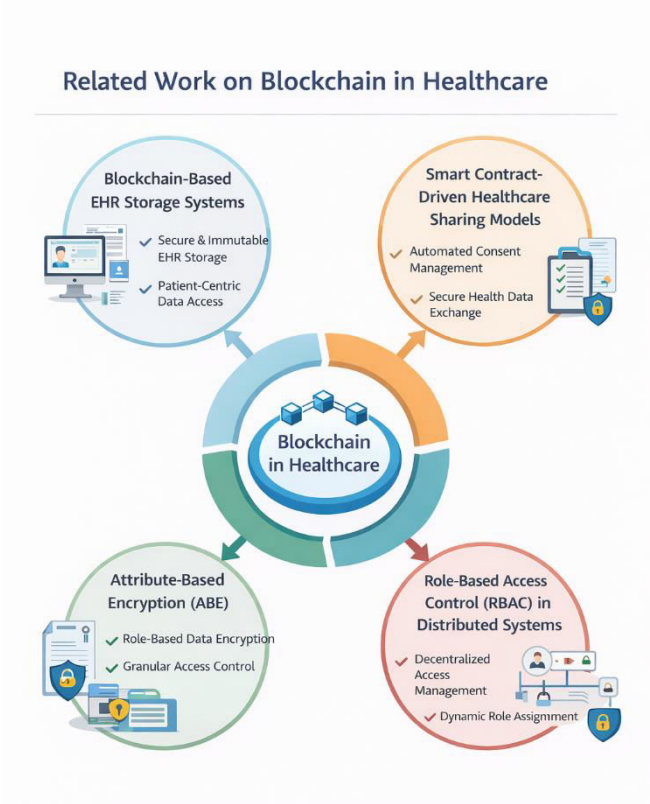
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504242|



III. PROBLEM STATEMENT

Despite advancements in healthcare digitization, existing medical record systems face multiple security and operational challenges. Centralized databases are susceptible to hacking, insider misuse, and accidental data modification. Patients often have minimal control over who accesses their records, and tracking unauthorized access can be difficult due to insufficient auditing mechanisms.

Furthermore, traditional access control models such as Role-Based Access Control (RBAC) lack flexibility in complex healthcare environments where access requirements may depend on multiple attributes such as department, specialization, emergency status, and patient consent.

Therefore, there is a need for a decentralized, secure, and scalable framework that ensures tamper-proof storage, dynamic fine-grained access control, and transparent auditability while preserving patient privacy.

IV. PROPOSED SYSTEM

The proposed system introduces a permissioned blockchain network where only verified healthcare institutions, doctors, and authorized stakeholders can participate. The architecture consists of three major components: blockchain layer, off-chain storage layer, and application layer.

Medical records are encrypted using Advanced Encryption Standard (AES) before being stored in secure off-chain storage such as cloud or IPFS. The blockchain stores only the hash value of the record along with metadata, ensuring data integrity without overloading the network. Smart contracts manage access permissions and enforce authorization rules automatically.

Fine-grained access control is implemented using an Attribute-Based Access Control (ABAC) model. Access decisions are made based on user attributes such as role, department, designation, and patient consent. Every access request is logged immutably on the blockchain, ensuring full transparency and auditability.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504242|

V. METHODOLOGY

The methodology begins with designing a secure blockchain architecture suitable for healthcare environments. A permissioned blockchain model is selected to restrict participation to authorized entities. Smart contracts are developed to define and enforce access control rules.

Medical records undergo encryption using AES-256 before storage. A SHA-256 hashing algorithm generates a unique hash value for each record, which is then stored on the blockchain. When a user requests access, the smart contract verifies their attributes and permissions. If authorized, the encrypted data is retrieved and decrypted using appropriate keys.

System performance is evaluated based on transaction latency, scalability, and resistance to unauthorized access attempts. Security analysis is conducted to verify resistance against data tampering, replay attacks, and unauthorized modifications.

VI. IMPLEMENTATION

The proposed blockchain-based medical record management system is implemented using a layered architecture consisting of the blockchain layer, application layer, access control layer, and off-chain storage layer. A permissioned blockchain platform such as Hyperledger Fabric is selected to ensure that only authorized healthcare entities participate in the network. The network includes peers representing hospitals, diagnostic centers, and regulatory authorities. A certificate authority (CA) is used to issue digital identities to users and organizations, ensuring authenticated participation.

User Registration and Identity Management

Each participant in the system (patients, doctors, nurses, administrators, and researchers) is registered through a secure identity management module. During registration, user attributes such as role, department, specialization, and access clearance level are verified. A unique cryptographic key pair (public and private key) is generated for each user. The public key is stored on the blockchain, while the private key is securely maintained by the user for authentication and digital signatures.

Attribute information is embedded into the blockchain network through smart contracts to enable fine-grained access validation. This ensures that access decisions are based not only on user roles but also on contextual attributes.

Smart Contract Development

Smart contracts (chaincode in Hyperledger or Solidity in Ethereum) are developed to manage access control policies and transaction validation. These contracts define

- Data upload procedures
- Access request verification
- Consent management rules
- Access revocation mechanisms
- Logging and auditing functions

When a user requests access to a medical record, the smart contract automatically checks predefined access policies. The contract verifies whether the user's attributes match the required conditions (e.g., department = cardiology AND role = doctor). If conditions are satisfied, access permission is granted; otherwise, the request is denied and recorded in the ledger.

Medical Record Upload Process

When a patient's medical record is created or updated, the following steps occur:

1. The medical file (e.g., PDF, scan report, prescription) is encrypted using AES-256 encryption.
2. A SHA-256 hash of the encrypted file is generated.
3. The encrypted file is stored in off-chain storage such as IPFS or secure cloud storage.
4. The hash value, metadata (timestamp, owner ID, file type), and storage reference are stored on the blockchain.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

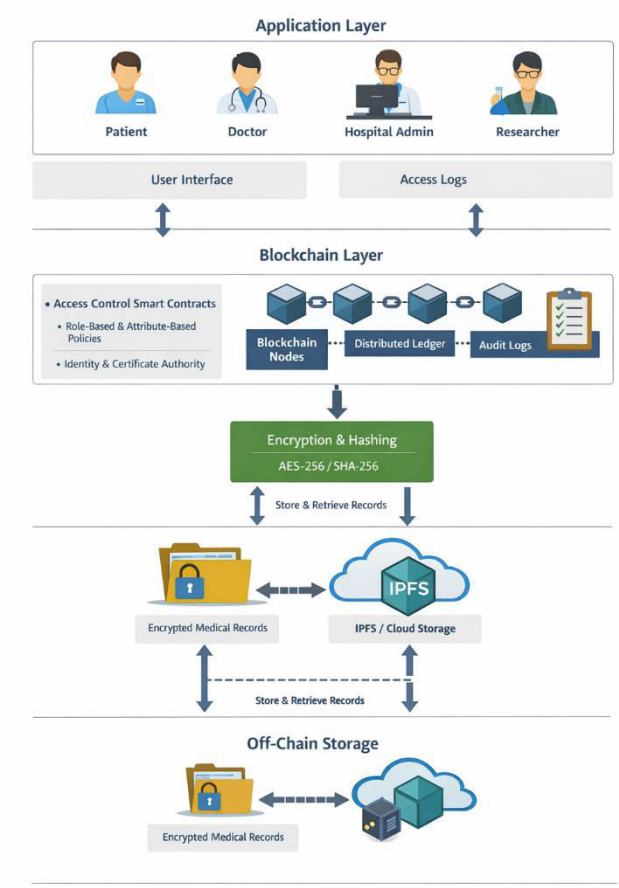
|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504242|

5. A transaction is recorded in the ledger to ensure immutability.

Storing only the hash on-chain reduces storage overhead and improves scalability while maintaining data integrity.



ETHICAL CONSIDERATION

Handling medical data requires strict adherence to ethical and regulatory standards. Patient privacy, confidentiality, and informed consent are fundamental principles in healthcare data management. The proposed framework ensures that patients maintain control over their records and can grant or revoke access permissions at any time.

The system maintains transparency through immutable logs while preventing unnecessary data exposure through encryption and attribute-based restrictions. Compliance with healthcare data protection regulations such as HIPAA and GDPR principles is considered in system design. Ethical deployment also requires fairness, accessibility, and responsible use of patient data.

VII. RESULTS AND DISCUSSION

Experimental evaluation shows that the proposed blockchain framework significantly improves data integrity and transparency compared to traditional centralized systems. Unauthorized access attempts are effectively prevented through smart contract validation. The system demonstrates acceptable transaction latency within healthcare operational requirements.

Off-chain storage reduces blockchain load and enhances scalability. Immutable audit trails increase trust among stakeholders by providing verifiable evidence of data access history. While blockchain introduces slight computational overhead, the security and transparency benefits outweigh the performance trade-offs.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504242|

VIII. CONCLUSION AND FUTUREWORK

This paper presents a comprehensive blockchain-based framework for secure medical record management integrated with fine-grained access control. By combining permissioned blockchain architecture, smart contracts, encryption, and attribute-based authorization, the system enhances data security, privacy, and patient empowerment.

Future work may focus on integrating artificial intelligence for predictive healthcare analytics, incorporating IoT-based health monitoring devices, optimizing scalability using Layer-2 solutions, and enabling interoperability with national healthcare systems. Further real-world deployment studies will strengthen validation of the proposed model.

REFERENCES

1. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
2. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “MedRec: Using Blockchain for Medical Data Access and Permission Management,” in Proceedings of IEEE Open & Big Data Conference, 2016.
3. P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, “FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data,” Computational and Structural Biotechnology Journal, vol. 16, pp. 267–278, 2018.
4. M. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, “BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments,” Information, vol. 8, no. 2, 2017.
5. K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, “MedBlock: Efficient and Secure Medical Data Sharing via Blockchain,” Journal of Medical Systems, vol. 42, no. 8, 2018.
6. Hyperledger Fabric Documentation, “Hyperledger Fabric Architecture,” The Linux Foundation, 2023.
7. V. Buterin, “Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform,” Ethereum White Paper, 2014.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details