Design and Implementation of a Prototype Blockchain-Based Secure Medical Record System with Family Health History Linking

Apurv Musandi[1], Shashikant Patil[2], Pranav Gouraje[3]
[123]*Department of Computer Science and Engineering,*
Sharad Institute of Technology College of Engineering, Ichalkaranji, Maharashtra, India

***Abstract*-- The increasing reliance on digital healthcare systems has intensified concerns regarding data security, privacy, and integrity in Electronic Health Record (EHR) management. Conventional centralized healthcare databases are susceptible to single-point failures, unauthorized data modification, and limited patient control over sensitive medical information. This paper presents the design and implementation of a prototype blockchain-based secure medical record system that integrates encrypted off-chain storage with on-chain integrity verification. The proposed framework utilizes Ethereum smart contracts to manage access permissions and store cryptographic hashes of medical records, while actual encrypted medical data is securely maintained in a cloud-based database. A distinctive feature of the system is the incorporation of family health history linking, enabling structured association of related patient records to support hereditary disease traceability without exposing confidential medical details. The hybrid architecture ensures scalability, enhanced security, and patient-controlled access while maintaining data integrity through blockchain validation. Experimental deployment on a public Ethereum test network demonstrates the feasibility and practical applicability of the proposed system for secure and decentralized healthcare data management.**

***Index Terms*— Blockchain, Electronic Health Records, Family Health Linking, Smart Contracts, Data Encryption, Decentralized Healthcare.**

I. INTRODUCTION

The digital transformation of healthcare systems has significantly improved the efficiency of medical record management and clinical data accessibility. Electronic Health Records (EHRs) have replaced traditional paper-based systems, enabling hospitals and healthcare providers to store, retrieve, and share patient information electronically. Despite these advancements, most existing EHR infrastructures are built upon centralized database architectures. Centralized systems rely on a single governing authority for data storage and access control, making them vulnerable to cyber-attacks, data breaches, insider manipulation, and single-point failures. The growing number of healthcare data breaches worldwide highlights the urgent need for more secure and transparent medical record management mechanisms.

In addition to security concerns, centralized systems often limit patient autonomy. Patients typically have minimal control over who accesses their medical data, how it is shared, and how long it is retained. This lack of transparency reduces trust between patients and healthcare providers. Furthermore, interoperability between hospitals remains a challenge due to heterogeneous database structures and differing administrative policies.

Blockchain technology has emerged as a promising solution to address these limitations. Blockchain is a decentralized and distributed ledger system that ensures immutability, transparency, and cryptographic security of stored transactions. In blockchain-based healthcare systems, smart contracts can be utilized to automate access control policies and ensure that medical data cannot be altered without detection. However, directly storing large medical files on blockchain networks is impractical due to storage constraints and high transaction costs.

To overcome these challenges, hybrid architectures combining on-chain verification with off-chain encrypted storage have been proposed. While such models improve data integrity and scalability, most existing implementations primarily focus on secure storage and permission management. Limited research has explored structured family health history linkage within blockchain-based systems. Family medical history plays a crucial role in identifying hereditary disease risks and long-term health patterns, yet current digital health systems rarely incorporate secure mechanisms for linking related patient records.

This paper proposes the design and implementation of a prototype blockchain-based secure medical record system that integrates encrypted cloud storage, smart contract-driven access control, and family health history linking within a unified framework. The proposed hybrid architecture ensures tamper-proof record verification while maintaining scalability, privacy, and patient-controlled accessibility. The system is deployed on a public Ethereum test network to validate feasibility and demonstrate practical applicability in modern healthcare environments.

II. LITERATURE REVIEW

The integration of blockchain technology in healthcare has gained significant attention in recent years due to its potential to enhance data security, interoperability, and patient-centred access control. Traditional Electronic Health Record (EHR) systems rely primarily on centralized database architectures, which expose healthcare infrastructures to risks such as single-point failures, unauthorized data modification, and cyber-attacks. Recent studies have explored blockchain as a decentralized alternative to improve data integrity and transparency in healthcare environments.

Chen et al. [1] proposed a blockchain-based secure medical data sharing system that utilizes smart contracts for access management and ensures data immutability through cryptographic hashing. Their work demonstrates the feasibility of storing record hashes on-chain while maintaining medical files off-chain to address storage limitations. Similarly, Dubovitskaya et al. [2] developed a blockchain framework for secure medical data exchange among multiple healthcare entities. Their architecture emphasizes interoperability and auditability but primarily focuses on institutional data sharing rather than patient-controlled record management.

A systematic review conducted by Agbo et al. [3] analyzed various blockchain healthcare implementations and identified scalability and regulatory compliance as major challenges. The study highlights the importance of hybrid architectures that combine blockchain verification with off-chain encrypted storage. More recent research by Kumar and Tripathi [4] (2023) explored Ethereum-based smart contracts for secure EHR access control, demonstrating improved transparency but noting the absence of structured family health relationship modeling within existing systems.

In the Indian context, the Ayushman Bharat Digital Mission (ABDM) introduced the ABHA (Ayushman Bharat Health Account) framework to provide unique digital health identifiers and enable interoperability across healthcare providers. While ABHA improves digital health identity management and centralized record access, it primarily operates under federated or centralized data governance models. The system relies on trusted authorities for record exchange and does not inherently provide immutable distributed ledger validation as offered by blockchain-based systems. Therefore, although ABHA enhances accessibility and national-level interoperability, it does not eliminate centralized trust dependencies or fully address tamper-proof integrity verification.

Furthermore, existing blockchain-based EHR solutions predominantly focus on secure storage and access permissions. Limited research has addressed the integration of family health history linkage within blockchain architectures. Family medical history plays a crucial role in identifying hereditary disease predispositions, yet current implementations treat patient records as isolated entities without secure relational linkage mechanisms.

Based on the review of recent blockchain healthcare literature and national digital health initiatives, a research gap is identified in the development of a hybrid blockchain prototype that integrates encrypted off-chain storage, smart contract-based access control, and structured family health history linking within a unified and deployable framework. The proposed system aims to address this gap by implementing a

practical architecture deployed on a public Ethereum test network.

III. PROPOSED SYSTEM

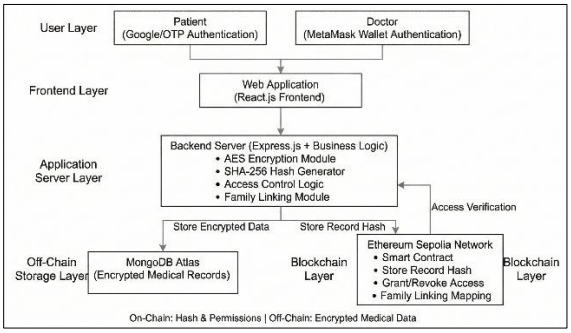

Fig. 1. Hybrid blockchain-based medical record system architecture.

The proposed system presents a hybrid blockchain-based architecture for secure medical record management integrating encrypted off-chain storage, smart contract-driven access control, and structured family health history linkage. The system is designed as a prototype framework deployed on a public Ethereum test network to demonstrate practical feasibility and security enhancement over centralized healthcare models.

The architecture consists of four primary layers: User Interface Layer, Application Server Layer, Off-Chain Storage Layer, and Blockchain Layer. Fig.1 illustrates the overall system architecture.

At the User Interface Layer, patients and doctors interact with the system through a web-based frontend developed using modern client-side technologies. Patients authenticate using secure identity mechanisms, while doctors utilize blockchain wallet authentication to establish cryptographic identity. The interface allows patients to grant or revoke access permissions and enables doctors to upload medical records upon authorization.

The Application Server Layer handles business logic, encryption processes, and blockchain interaction. When a doctor uploads a medical record, the server generates a symmetric encryption key and encrypts the medical data using Advanced Encryption Standard (AES). The encrypted record is then stored in a cloud-based MongoDB database. A cryptographic hash of the encrypted data is generated using SHA-256 to ensure integrity verification.

The Off-Chain Storage Layer stores encrypted medical records to overcome blockchain storage limitations and transaction costs. Storing large medical files directly on-chain is impractical due to scalability constraints; therefore, the proposed hybrid approach ensures efficient storage while preserving security.

The Blockchain Layer, implemented using Ethereum smart contracts, stores cryptographic hashes of medical records and manages access permissions. Smart contracts maintain mappings between patients and authorized doctors. Once a record hash is stored on-chain, it becomes immutable and tamper-evident. Any modification to the off-chain record results in a hash mismatch, thereby enabling integrity validation.

A distinctive feature of the proposed system is the Family Health History Linking mechanism. Through smart contract functions, patients can securely link their records with related family members. This linkage allows controlled visibility of hereditary medical information without exposing full medical datasets. The family linking structure enhances long-term clinical analysis and supports hereditary disease traceability while maintaining privacy.

The hybrid on-chain and off-chain architecture ensures scalability, data confidentiality, and tamper-proof validation, making the system suitable for modern digital healthcare ecosystems.

IV. METHODOLOGY

The proposed system follows a hybrid on-chain and off-chain architecture to ensure data confidentiality, integrity, scalability, and controlled accessibility. The methodology is structured into five major components: authentication mechanism, encryption process, off-chain data storage, blockchain-based integrity verification, and family health linkage implementation.

A. Authentication Mechanism

The system implements a dual authentication model to accommodate different user roles. Patients authenticate through secure identity verification mechanisms integrated within the web application layer, while doctors authenticate using blockchain wallet-based cryptographic identity. MetaMask is utilized as a wallet provider to establish a unique public-private key pair for doctors. Transaction

signing ensures non-repudiation and prevents unauthorized smart contract interactions. This hybrid authentication approach enhances usability while maintaining cryptographic security for blockchain operations.

B. Encryption and Data Confidentiality

To protect sensitive medical information, the system employs symmetric key encryption using the Advanced Encryption Standard (AES-256). When a medical record is submitted by an authorized doctor, the backend server generates a unique symmetric encryption key. The plaintext medical data is encrypted before being transmitted to the off-chain storage layer.

Let M represent the medical record data and K represent the generated encryption key. The encrypted record C is computed as:

C = AES_Encrypt(M, K)

This ensures that even if the database is compromised, the stored data remains unintelligible without the corresponding decryption key. The encryption process is executed at the server layer prior to database storage to prevent exposure during transmission.

C. Off-Chain Storage Strategy

Due to the storage limitations and transaction costs associated with blockchain networks, storing large medical files directly on-chain is impractical. Therefore, encrypted medical records are stored in a cloud-based MongoDB database. The off-chain storage mechanism ensures scalability and efficient retrieval while preserving confidentiality through encryption.

Each stored record contains:
• Encrypted medical data
• Timestamp
• Associated patient identifier
• Metadata reference

This hybrid model reduces blockchain congestion and ensures performance efficiency.

D. Hash Generation and Integrity Verification

To guarantee tamper-proof validation, the system generates a SHA-256 cryptographic hash of the encrypted record. The hash value H is computed as:

H = SHA256(C)

The generated hash is then stored on the Ethereum blockchain through a smart contract function. Since blockchain data is immutable, any modification to the encrypted record in the database would produce a different hash value, thereby enabling integrity verification.

During record retrieval, the system recalculates the SHA-256 hash of the stored encrypted data and compares it with the hash stored on-chain. A mismatch indicates potential tampering, ensuring transparent and verifiable data integrity.

E. Smart Contract-Based Access Control

The blockchain layer is implemented using Ethereum smart contracts written in Solidity. The smart contract maintains mappings between patient addresses and authorized doctor addresses. Access permissions are enforced programmatically through functions such as grantAccess() and revokeAccess().

Only doctors with granted permission can invoke the function to store a new record hash on-chain. Each blockchain transaction includes:
• Patient blockchain address
• Record hash
• Timestamp
• Doctor blockchain address

The use of smart contracts eliminates reliance on centralized authorities for permission validation. The interaction workflow for secure medical record upload and blockchain verification is illustrated in Fig. 2.

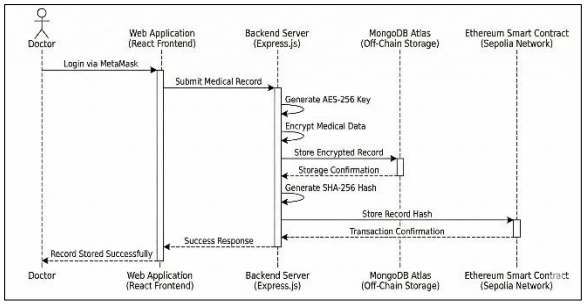

Fig. 2. Sequence diagram for secure medical record upload and blockchain integrity verification.

F. Family Health History Linking

A distinctive feature of the proposed methodology is the structured family health history linkage

mechanism. The smart contract includes a relational mapping that associates blockchain addresses of related individuals. Through explicit consent, a patient can link their address with a parent, child, or sibling.

This linkage does not expose full medical data but enables controlled visibility of hereditary health information. The approach supports early detection of genetic predispositions while preserving privacy through encryption and permission-based access control.

G. Deployment and Network Configuration

The prototype system is deployed on the Ethereum Sepolia test network to validate real-world feasibility. Smart contracts are compiled and deployed using the Hardhat development framework. Blockchain interactions from the backend are facilitated using the Ethers.js library. The off-chain storage layer is hosted on MongoDB Atlas cloud infrastructure.

This deployment strategy ensures that the system operates within a realistic decentralized environment while maintaining cost efficiency during testing.

Overall, the methodology integrates cryptographic encryption, decentralized integrity verification, and structured access control within a unified hybrid architecture. The combination of AES encryption, SHA-256 hashing, Ethereum smart contracts, and cloud storage provides a scalable and secure framework suitable for modern healthcare applications.

V. RESULTS AND ANALYSIS

The proposed prototype system was implemented and tested to evaluate functional correctness, security performance, and architectural feasibility. The system integrates a blockchain-based smart contract deployed on the Ethereum Sepolia test network, encrypted off-chain storage using MongoDB Atlas, and a web-based user interface for interaction.

A. Functional Validation

The following functional scenarios were successfully tested:

1. Doctor authentication using blockchain wallet identity.
2. Patient authorization and access permission management.
3. Encryption of medical records prior to database storage.
4. Generation and storage of SHA-256 record hash on blockchain.
5. Integrity verification through hash comparison.
6. Family health linkage between related patient accounts.

Each operation produced valid transaction confirmations on the Sepolia network. The smart contract recorded immutable hash values, and transaction logs were verifiable through blockchain explorers, confirming successful deployment and execution.

B. Security Evaluation

The security of the proposed system was evaluated based on confidentiality, integrity, access control, and tamper resistance.

1. Confidentiality:

Medical records are encrypted using AES-256 before being stored in MongoDB. Without access to the encryption key, raw database data remains unreadable. This ensures protection against unauthorized database-level access.

2. Integrity:

SHA-256 hashing guarantees tamper detection. Any modification in the encrypted record alters the computed hash value. Since the original hash is permanently stored on blockchain, mismatched hashes indicate unauthorized changes.

3. Access Control:

Smart contracts enforce permission validation. Only doctors with granted access can submit medical record hashes. Unauthorized users attempting to invoke restricted functions are rejected at the blockchain layer.

4. Decentralized Verification:

Because record hashes are stored on Ethereum, integrity validation does not depend on a centralized authority. This eliminates single-point failure risk in verification processes.

C. Performance Observations

The off-chain storage approach significantly reduces blockchain transaction overhead. Only small hash values are stored on-chain, minimizing gas costs and improving scalability. Storing full medical files directly on blockchain would increase transaction latency and cost; the hybrid architecture resolves this limitation.

Blockchain transaction confirmation time on Sepolia averaged between 10–30 seconds depending on network conditions. Off-chain database storage and encryption processes executed within milliseconds at the application server level, ensuring responsive system performance.

D. Comparative Analysis

To evaluate the effectiveness of the proposed system, a comparison was conducted between traditional centralized healthcare systems, the ABHA-based centralized digital health framework, and the proposed hybrid blockchain architecture.

Table I Comparison of Centralized System, ABHA Framework, and Proposed System

Feature	Centralized System	ABHA Framework	Proposed System
Data Storage Model	Fully Centralized Database	Federated / Centralized Infrastructure	Hybrid (Blockchain + Encrypted Off-Chain Storage)
Data Integrity Mechanism	Database-Level Logging	Central Authority Validation	Blockchain-Based Hash Verification(SHA-256)
Tamper Resistance	Limited	Moderate	High (Immutable Smart Contract)
Patient Access Control	Role-Based (Hospital Controlled)	Identity-Based via ABHA	Smart Contract-Controlled Permission Mapping
Family Health Linking	Not Supported	Not Structured	Structured Blockchain-Based Family Mapping
Single Point of Failure	Present	Partially Present	Eliminated via Decentralized Verification
Data Encryption Before Storage	Optional/ Implementation Dependent	Implemented at System Level	AES-256 Encryption Before Off-Chain Storage
Transparency and Auditability	Limited Internal Logs	Government-Controlled Audit Trails	Publicly Verifiable On-Chain Hash Records

E. Discussion

The comparative analysis demonstrates that centralized healthcare systems remain vulnerable to internal manipulation and single-point failures. While the ABHA framework improves digital health identity management and interoperability, it still relies on trusted authorities for validation. In contrast, the proposed system ensures decentralized integrity verification through blockchain while maintaining scalability via encrypted off-chain storage.

The inclusion of family health history linkage further differentiates the proposed model from existing blockchain EHR systems. By enabling consent-based relational mapping between patient accounts, the system supports hereditary disease traceability without compromising sensitive medical information.

The experimental deployment confirms the feasibility of integrating blockchain technology within healthcare record management while preserving performance efficiency and user accessibility.

VI. THREAT MODEL AND LIMITATIONS

The security of the proposed hybrid blockchain-based medical record system is evaluated under a defined threat model that considers realistic adversarial scenarios within healthcare infrastructures. The system assumes that attackers may attempt to compromise database storage, intercept communication channels, or perform unauthorized access attempts at the application layer.

A. Threat Model

1. Database Compromise Scenario
   In the event that the off-chain database is compromised, the attacker may gain access to encrypted medical records. However, due to AES-256 encryption applied before storage, the attacker cannot interpret the medical data without access to the corresponding encryption key. Furthermore, integrity validation through

SHA-256 hash comparison with the blockchain prevents undetected record modification.

2. Data Tampering Attempt
   If an adversary attempts to modify stored encrypted medical records in MongoDB, the recalculated hash value will not match the original hash stored on the Ethereum blockchain. Since blockchain entries are immutable, any alteration becomes immediately detectable during integrity verification.
3. Unauthorized Access Attempt
   Access control is enforced through smart contract permission mapping. Unauthorized users cannot submit medical record hashes or access restricted data without being granted explicit permission by the patient. Transactions failing access validation are rejected at the blockchain layer.
4. Replay or Impersonation Attacks
   Doctor authentication via blockchain wallet ensures cryptographic identity verification. Each transaction is digitally signed using the private key associated with the wallet, preventing impersonation without possession of the private key.

B. System Assumptions

The system assumes that the Ethereum blockchain network remains secure under standard decentralized consensus mechanisms. It also assumes secure key management at the user level and proper protection of private keys in wallet applications.

C. Limitations

Despite its advantages, the proposed system has certain limitations:

1. Blockchain Latency
   Public blockchain networks introduce transaction confirmation delays depending on network congestion. Although acceptable for medical record validation, this latency may not be suitable for real-time emergency scenarios.
2. Key Management Complexity
   Loss of private keys associated with blockchain wallets may restrict access to blockchain-controlled permissions. Secure key recovery mechanisms require further research.
3. Scalability Constraints
   While off-chain storage improves scalability, large-scale deployment across national healthcare systems would require optimization of indexing, caching, and distributed infrastructure.
4. Regulatory and Integration Challenges
   Integration with national digital health frameworks such as ABHA would require compliance with regulatory policies and interoperability standards.

Future improvements may incorporate advanced privacy-preserving mechanisms such as zero-knowledge proofs, decentralized identity frameworks, and optimized layer-2 blockchain scaling solutions.

VII. CONCLUSION

The proposed study presented the design and implementation of a prototype blockchain-based secure medical record management system integrating encrypted off-chain storage with on-chain integrity verification. The hybrid architecture combines AES-256 encryption for data confidentiality, SHA-256 hashing for integrity validation, and Ethereum smart contracts for decentralized access control. Unlike traditional centralized healthcare systems and federated digital health frameworks, the proposed model eliminates single-point failure in integrity verification and enhances transparency through immutable ledger records.

A key contribution of this work is the structured family health history linking mechanism, which enables controlled association of related patient accounts without exposing sensitive medical data. This feature enhances clinical relevance by supporting hereditary disease traceability while maintaining privacy through cryptographic protection.

Experimental deployment on the Ethereum Sepolia test network demonstrates the feasibility of integrating blockchain technology with cloud-based storage in healthcare environments. The results

confirm that the hybrid approach provides improved security, tamper resistance, and patient-controlled accessibility compared to centralized architectures.

Future work may focus on scalability optimization, integration with national digital health ecosystems, incorporation of zero-knowledge proof techniques for enhanced privacy, and performance benchmarking under large-scale healthcare datasets.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to Mrs. Ashwini Kalaje(Project Guide, CSE Department, Sharad Institute of Technology College of Engineering) for her continuous guidance, valuable suggestions, and academic support throughout the development of this project. Her mentorship significantly contributed to the successful completion of this research work.

Additionally, the authors acknowledge the support of the Department of Computer Science and Engineering, Sharad Institute of Technology College of Engineering, Ichalkaranji, for providing the necessary resources and academic environment to carry out this study.

REFERENCES

[1] S. Chen, R. Shi, Z. Ren, J. Yan, Y. Shi, and J. Zhang, "A blockchain-based medical data sharing and protection scheme," IEEE Access, vol. 7, pp. 118943–118953, 2019.

[2] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," AMIA Annual Symposium Proceedings, 2017.

[3] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: A systematic review," Healthcare, vol. 7, no. 2, 2019.

[4] R. Kumar and A. Tripathi, "Blockchain-based secure electronic health record management using smart contracts," International Journal of Information Security and Privacy, vol. 17, no. 1, pp. 1–18, 2023.

[5] National Health Authority, "Ayushman Bharat Digital Mission (ABDM) – ABHA overview," Government of India, 2022.