CYBERSECURITY USING BLOCKCHAIN TECHNOLOGY

Roopa DE[1] , Prajwal Kurdekar[2], Ganesh GH[3], Anish Patil[4], Darshan MS[5]

1 Assistant Professor, Information Science and Engineering, Bapuji Institute of Engineering and technology, Karnataka, India

2 Bachelor of Engineering, Information Science and Engineering, Bapuji Institute of Engineering and technology, Karnataka, India

3 Bachelor of Engineering, Information Science and Engineering, Bapuji Institute of Engineering and technology, Karnataka, India

4 Bachelor of Engineering, Information Science and Engineering, Bapuji Institute of Engineering and technology, Karnataka, India

5 Bachelor of Engineering, Information Science and Engineering, Bapuji Institute of Engineering and technology, Karnataka, India.

Abstract

The rapid digitization of clinical information has intensified the necessity for advanced protection mechanisms to secure patient data. This study introduces a robust EHR security model that integrates authenticated symmetric encryption with a permissioned blockchain, ensuring confidentiality and tamper-proof integrity guarantees. Individual medical records are encrypted using AES-GCM and stored securely off-chain, while compact integrity digests are anchored on a Hyperledger Fabric ledger to identify unauthorized alterations. A hierarchical key-wrapping scheme governs access privileges, releasing decryption keys solely to verified stakeholders. Furthermore, the system records comprehensive access logs to facilitate future anomaly-detection models. Together, these components establish a verifiable, auditable, and scalable methodology for safeguarding clinical data, forming the foundation for intelligent threat-monitoring capabilities.

Index Terms— Blockchain, Electronic Health Records, AES-GCM, Hyperledger Fabric, Integrity Verification, Anomaly Detection, Machine Learning Security.

I. INTRODUCTION

Electronic health systems form a vital technological backbone in healthcare institutions. However, many existing EHR systems rely on centralized repositories, making sensitive patient information vulnerable to unauthorized exposure, manipulation, or system-wide breaches. Since medical documents carry highly personal identifiers and health details, even minor security lapses can create significant legal, clinical, and ethical risks. As a result, modern EHR infrastructures must ensure confidentiality, tamper-evidence, and enforce strict accountability.

This work proposes a hybrid security framework that employs AES-GCM authenticated encryption in conjunction with a private Hyperledger Fabric blockchain. Each patient's record is independently encrypted and preserved in off-chain storage. The encrypted file's hash is then committed to Fabric to act as an immutable integrity reference. A hierarchical key-management mechanism governs decryption rights, enabling controlled access for authorized roles. Moreover, fine-grained system logs are maintained to support machine-learning-based anomaly analysis.

The major contributions of this study include:

1. A secure AES-GCM workflow for confidentiality and verification of medical PDFs.
2. The use of Hyperledger Fabric to maintain tamper-evident integrity proofs.
3. A layered key-wrapping system enabling controlled, role-based data access.
4. Comprehensive audit logs designed for future ML-driven anomaly detection.

II. RELATED WORK

Research on securing electronic health data primarily spans three domains: blockchain-enabled EHR systems, cryptographic protection methods, and machine-learning-driven anomaly detection.
The following subsections summarize key findings in each domain.

A. Blockchain-Enabled Healthcare Platforms

Blockchain has been widely studied as a means to ensure immutable provenance and traceability within healthcare systems. Proposed models generally fall into three design categories:

1. **On-Chain Storage:** Directly storing medical data on public blockchains like Ethereum ensures immutability but suffers from excessive storage cost, limited throughput, and privacy challenges due to public visibility.

2. **Hybrid Storage Models:** To preserve scalability, sensitive files are stored off-chain (e.g., cloud storage, IPFS), while their hashes are anchored on-chain. This reduces blockchain load while maintaining tamper-evidence.

3. **Permissioned/Consortium Blockchains:** Platforms like Hyperledger Fabric allow controlled participation, configurable access policies, and higher throughput. Our system adopts this design for integrity preservation.

B. Cryptographic Security in EHR Systems

Core security functions rely on proven cryptographic mechanisms:

1. **Symmetric Encryption:** AES-GCM is favored for its support of authenticated encryption, producing both encrypted output and an integrity tag.

2. **Key Wrapping and PKI:** Hierarchical key management enables generation of per-patient keys that are secured under a master key, supporting granular access control.

3. **Hashing and Digital Signatures:** SHA-256 is commonly used to generate compact integrity proofs stored on blockchain for future comparison.

C. Anomaly Detection in EHR Usage

Even secure systems remain susceptible to insider misuse. Hence, anomaly-detection research focuses on analyzing behavioral logs.

1. **Unsupervised Models:** Tools such as Isolation Forest, Autoencoders, and One-Class SVM are effective in highlighting unusual access patterns.

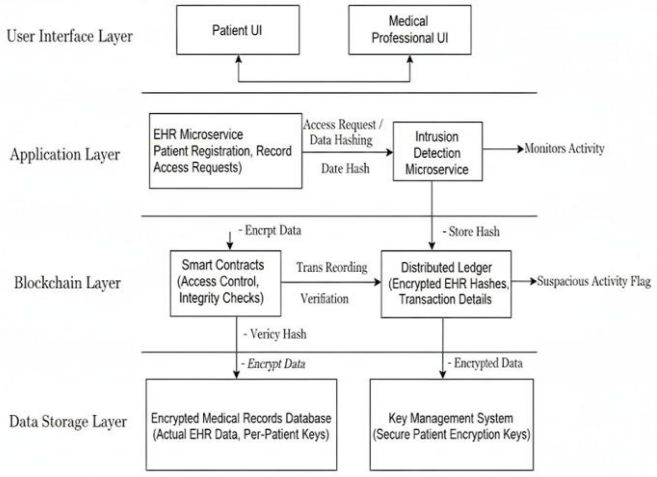
2. **Behavioral Threat Modelling:** Access logs are transformed into structured feature sets and monitored for deviations. Our system collects similar logs to enable such intelligence in the future.

D. Comparative Analysis of Existing Approaches

Current EHR models present trade-offs:
• Fully on-chain systems are costly and privacy-invasive.
• Pure cloud systems lack immutable protection.
• Encryption alone cannot detect tampering.
• Blockchain systems without behavioral analytics miss insider threats.

Our architecture integrates all three: encryption, blockchain immutability, and ML-ready logging.

III. SYSTEM ARCHITECTURE



The proposed architecture is divided into four operational layers:

1. **Frontend Layer (React):** Provides interfaces for uploading, retrieving, and verifying medical records.

2. **Backend Layer (Node.js Services):** Manages AES-GCM encryption, decryption, hashing, access logging, and blockchain communication.

3. **Blockchain Layer (Hyperledger Fabric):** Stores integrity hashes and enforces chaincode-based access policies.

4. **Secure Storage and Key-Management Layer:** Stores encrypted PDFs and manages per-patient key wrapping under a master key or HSM.

Upon uploading a file, the backend encrypts the PDF, generates a SHA-256 digest, stores the encrypted version in secure storage, and commits the hash to Fabric. When retrieval is requested, the patient-specific key is unwrapped for authorized users, and the decrypted result is validated by recomputing the hash.

IV. IMPLEMENTATION AND USER-FOCUSED SUBSYSTEMS

A functional prototype was developed with a React interface and a Node.js backend integrated with a Hyperledger Fabric test network.

A. Secure Encryption and Key Management

AES-GCM secures every medical document, ensuring both confidentiality and integrity tagging. Each patient is assigned a unique symmetric key. These keys are wrapped under a central master key and unwrapped strictly based on role-based permissions.

B. User-Centric Functional Modules

Key operational tools include:

- **Integrity Verification Module:** Users can validate a record by recomputing its hash and comparing it against the blockchain entry.

- **Audit Logging Engine:** All critical events—including uploads, access requests, decryptions, key unwrapping, and emergency overrides—are logged for future anomaly-detection integration.

V. EXPERIMENTAL EVALUATION AND RESULTS

The system was validated through unit tests, subsystem integration checks, and scenario-driven evaluations.

A. Qualitative Scenario Testing

A total of 48 test scenarios were executed, with 47 completing successfully (97.9% reliability). Observed results include:

- Successful encryption and on-chain hash entry during upload.

- Authorized decryption strictly enforced by role-based rules.

- Altered encrypted files were correctly identified as tampered.

- Emergency access mode functioned as intended while logging the override.

B. Quantitative Performance Measurements

Performance was assessed using representative 1–2 MB PDFs.
The results are shown below:

Metric	Time	Description
AES-GCM Encryption	8–12 ms	Secure file encryption
SHA-256 Hashing	3–5 ms	Integrity computation
Fabric Commit Time	150–180 ms	Ledger transaction
Decryption Time	8–10 ms	Authorized file retrieval
Key Unwrapping	< 5 ms	Master key operation
Integrity Check Accuracy	100%	No mismatches

VI. DISCUSSION, LIMITATIONS & FUTURE ENHANCEMENTS

The hybrid architecture demonstrates strong performance and reliable security behavior. However, several limitations exist:

- Blockchain transaction times may fluctuate based on network conditions.

- The prototype uses a single encrypted-file store, which may bottleneck under large workloads.

- ML-based anomaly detection is not yet integrated.

- Full compatibility with healthcare standards such as HL7-FHIR is still under development.

Future improvements include integrating real-time anomaly-detection models, enabling distributed encrypted storage, optimizing Fabric channel configurations, and introducing hardware-backed key storage.

VII. CONCLUSION

This paper presents a secure EHR management framework that merges AES-GCM encryption, blockchain-based integrity anchoring, and hierarchical key management to provide a trustworthy environment for clinical data handling. The system ensures protected storage, verifiable integrity, controlled access, and thorough auditability—forming a strong foundation for future intelligent security monitoring in healthcare.