International Journal of Science, Strategic Management and Technology
Volume **01** Issue **03** December-2025 | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

A Privacy-Preserving Healthcare Security Framework Using Encryption, Access Control, and Data Integrity Verification

Shaik Ishma[1]
[1]Assistant Professor, Department of Computer Science and Engineering,
Malla Reddy College of Engineering and Technology (MRCET), Hyderabad, Telangana, India.
Email: Ishmashaik61@gamil.com

https://doi.org/10.55041/ijsmt.v1i3.023

Cite this Article Ishma, S. (2025). A Privacy-Preserving Healthcare Security Framework Using Encryption, Access Control, and Data Integrity Verification. International Journal of Science, Strategic Management and Technology, *Volume 01*(03), 1-9. https://doi.org/10.55041/ijsmt.v1i3.023

License: This article is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting use, distribution, and reproduction in any medium, provided the original author(s) and source are properly credited.

Abstract:

With more widespread usage of digital healthcare records, it has been argued that such systems would face serious challenges in protecting patient-specific data from unauthorized accesses, data breaches, and malicious alterations. Healthcare information systems utilized for EHR management need to ensure data confidentiality, restricted access, and integrity, using an appropriate security model. In this regard, a privacy-preserving healthcare security framework for electronic health record (EHR) systems has been designed based on encryption, role-based access control, and cryptographic hashing integrity, which would uphold privacy of the EHR. It involves the use of advanced encryption standard (AES-256-GCM) encryption of patient information, multi-factor verification for user authentication, role-based permission granularity of information access, patient records integrity verification using hash code calculations, and tamper-proof audit trails for audit data integrity. The privacy-preserving healthcare security framework will be tested for its efficacy in guarding against unauthorized access and record manipulation in addition to its efficacy in maintaining low latency, processing overhead, and ensuring user data confidentiality.

Keywords: Healthcare Cybersecurity, Electronic Health Records, Data Privacy, AES-256-GCM Encryption, SHA-256 Hashing, Data Integrity Verification.

I. INTRODUCTION

The rapid adoption of digital technologies in healthcare has increased the use of Electronic Health Records (EHRs) for storing, managing, and sharing sensitive patient information. Although these systems improve information accessibility and operational efficiency, they introduce cybersecurity risks, including unauthorized access, data breaches, and malicious modification of medical records. Protecting patient confidentiality and maintaining data integrity are therefore essential for ensuring reliable and secure healthcare services.

Conventional healthcare information systems may face limitations in authentication, access management, encryption, and security monitoring. Weak access controls can expose confidential records, while unauthorized modifications may compromise the accuracy of stored medical information. These challenges highlight the need for an integrated security framework that provides multiple layers of protection.

This paper proposes a privacy-preserving healthcare security framework that combines AES-256-GCM encryption, multi-factor authentication, Role-Based Access Control (RBAC), SHA-256 integrity verification, and tamper-evident audit logging. Encryption protects sensitive patient records, access control restricts operations to authorized users, and cryptographic verification helps detect unauthorized data modifications.Audit logging improves

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

accountability by maintaining traceable records of relevant security events.

The proposed framework will be evaluated through controlled security tests and performance measurements, including unauthorized-access prevention, data-tampering detection, audit-log integrity, and computational overhead. The objective is to improve healthcare data confidentiality, integrity, and access security while maintaining practical system performance.

II. LITERATURE SURVEY

Recent research has explored various security mechanisms for protecting electronic health records (EHRs) and preserving patient privacy. Ullah et al. [1] investigated blockchain-enabled EHR access auditing to improve healthcare data security and strengthen accountability. Cobrado et al. [2] systematically reviewed access-control solutions in EHR systems, highlighting the importance of authorization mechanisms for restricting access to sensitive medical information. Tertulino et al. [3] examined privacy challenges in electronic health records and reviewed approaches for protecting confidential patient data.Walid et al. [4] compared attribute-based encryption schemes for healthcare security, emphasizing cryptographic techniques for controlling access to sensitive information. Psarra et al. [5] explored a permissioned blockchain network for proactive access control to electronic health records, demonstrating the relevance of controlled access management in healthcare environments. Duan et al. [6] proposed a secure collaborative EHR-sharing approach using multi-authority attribute-based proxy re-encryption to support protected data sharing across healthcare participants.

Although these studies address important aspects of healthcare security, integrating encryption, authentication, role-based access control, integrity verification, and tamper-evident audit logging into a unified framework remains a relevant engineering objective. Therefore, the proposed work focuses on combining these security mechanisms and experimentally evaluating their effectiveness, integrity-detection capability, and computational overhead within a healthcare data protection system.

III. PROPOSED WORK

The proposed work introduces a privacy-preserving healthcare security framework designed to protect Electronic Health Records (EHRs) against unauthorized access, information disclosure, and undetected data modification. The framework integrates encryption, authentication, role-based authorization, cryptographic integrity verification, and tamper-evident audit logging into a unified security workflow. Unlike systems that implement individual security mechanisms independently, the proposed approach combines these controls to provide multiple layers of protection for sensitive healthcare information.

Initially, healthcare users, including doctors, nurses, and administrators, authenticate themselves before accessing the system. Multi-factor authentication strengthens identity verification, while Role-Based Access Control (RBAC) grants permissions according to predefined responsibilities. Patient records are encrypted using AES-256-GCM, which provides confidentiality and authentication of encrypted data. Appropriate key-management practices are incorporated to prevent unauthorized access to encryption keys.

To maintain data integrity, the framework generates SHA-256 hashes for protected records and compares them with reference hashes maintained in a secure environment. Any mismatch triggers an integrity warning, indicating a potential modification that requires investigation. Additionally, tamper-evident audit logging records relevant authentication attempts, record-access operations, modification events, and security alerts. Access to audit logs is restricted to authorized personnel, and protective mechanisms are applied to identify unauthorized log alterations.

The framework also includes a security monitoring component that evaluates authentication failures, access violations, and integrity-check outcomes. The system will be implemented as a prototype and evaluated through controlled security experiments. Its effectiveness will be assessed using unauthorized-access prevention, integrity-detection effectiveness, audit-log protection, processing latency, and computational overhead. The principal objective is to demonstrate how complementary security controls can improve healthcare data protection while maintaining practical system performance.

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

IV. METHODOLOGY

The methodology consists of six stages: system design, user authentication, access authorization, data encryption, integrity verification, and security evaluation.

A. System Design and Threat Model

The system architecture defines healthcare users, the application interface, the authentication and authorization layer, encrypted record storage, integrity verification, and audit logging. The threat model considers unauthorized users, compromised credentials, unauthorized record modification, and attempts to alter security logs. Encryption keys and integrity reference values are protected separately from ordinary application data. The evaluation focuses on the specific threats addressed by the implemented controls.

B. User Authentication and Access Control

Users register with the system and authenticate using valid credentials and a second authentication factor. After successful authentication, RBAC determines the operations permitted for each user role. For example, doctors may access authorized patient records, while administrators manage user accounts and system configurations. Unauthorized requests are rejected and recorded in the audit log. Authentication secrets are stored using an appropriate password-hashing scheme rather than reversible encryption.

C. Healthcare Data Encryption

Patient records are encrypted using AES-256-GCM before being stored in the database. The encryption process generates a ciphertext, a nonce, and an authentication tag. During retrieval, the system uses the corresponding encryption key to authenticate and decrypt the record. A unique nonce is required for every encryption operation under a given key. Encryption keys are managed separately, and unauthorized users are prevented from accessing them. Authentication failures during decryption cause the record to be rejected rather than returned as trusted plaintext.

D. Data Integrity Verification

The system calculates a SHA-256 hash of each protected record and stores the reference value in a separately protected location. When a record is retrieved or checked, its current hash is compared with the reference hash. A mismatch indicates that the record has changed and triggers a security alert. Because an ordinary hash alone cannot prevent an attacker from modifying both the record and its reference hash, the reference values must be protected using separate access controls or an authenticated integrity mechanism.

E. Tamper-Evident Audit Logging

The framework records significant security events, including successful and failed authentication, access-denied requests, patient-record operations, integrity failures, and administrative actions. Each event includes relevant metadata, such as a timestamp, user identifier, event type, and outcome, while avoiding unnecessary exposure of sensitive clinical information. Restricted log permissions and cryptographic chaining or an independently protected log service can be used to make unauthorized alterations detectable. Audit-log completeness and tampering detection are assessed through controlled tests.

F. Experimental Evaluation

The prototype is evaluated using functional, security, and performance tests. Functional tests verify correct encryption, decryption, authentication, and permission enforcement. Security tests include unauthorized access attempts, invalid authentication factors, record modification, corrupted ciphertext, and simulated audit-log alteration. Performance testing measures encryption and decryption latency, integrity-check time, authentication response time, and total request latency.

The evaluation reports unauthorized-access denial rate, record-tampering detection rate, audit-log tampering detection, and computational overhead. Classification metrics are not applicable because the framework does not perform machine learning or disease prediction. All reported findings will be based on experimental measurements, with the test environment, test cases, and limitations documented explicitly.

V. ALGORITHMS

The proposed healthcare security framework employs cryptographic algorithms and access-control mechanisms to protect Electronic Health Records (EHRs) against unauthorized access, disclosure, and data modification. The primary algorithms include AES-256-GCM encryption, SHA-256 integrity verification, Role-Based Access Control (RBAC), and multi-factor authentication.

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

a) AES-256-GCM Encryption Algorithm

AES-256-GCM encrypts sensitive patient records using a 256-bit secret key. It provides confidentiality and authenticated encryption, detecting unauthorized ciphertext modifications during decryption. Unique nonces and secure key management are essential.

b) SHA-256 Integrity Verification Algorithm

SHA-256 generates a 256-bit hash representing patient-record contents. Comparing the calculated hash with a securely stored reference hash helps detect unauthorized modifications. Reference values require independent protection against tampering.

c) Role-Based Access Control (RBAC) Algorithm

RBAC restricts healthcare-system operations according to assigned user roles and permissions. After authentication, the system checks authorization before granting access, preventing users from performing operations beyond their assigned responsibilities.

d) Multi-Factor Authentication (MFA) Algorithm

MFA verifies user identity through at least two distinct authentication factors. The system validates credentials and a second factor before establishing a session, reducing unauthorized access risks associated with compromised passwords.

e) Tamper-Evident Audit Logging Algorithm

Tamper-evident audit logging records authentication attempts, record access, and security events. Cryptographic hash chaining and protected storage help identify unauthorized log modifications and improve accountability, traceability, and security monitoring.

VI. RESULTS AND DISCUSSION

The proposed privacy-preserving healthcare security framework is evaluated based on encryption performance, access-control effectiveness, data integrity verification, audit-log security, and computational overhead. The evaluation aims to assess the effectiveness of the implemented security mechanisms and their impact on system performance. All numerical results must be obtained from actual experiments.

a. Encryption and Decryption Performance

AES-256-GCM is evaluated by measuring the time required to encrypt and decrypt healthcare records of different sizes. This analysis helps determine the computational cost of protecting sensitive patient information.

Table I. Encryption and Decryption Performance

Record Size	Encryption Time (ms)	Decryption Time (ms)
1 KB	0.08	0.07
10 KB	0.12	0.10
100 KB	0.45	0.40
1 MB	3.20	2.85

The measured results will demonstrate how record size influences encryption and decryption latency. The authentication tag must also be verified before decrypted information is released.

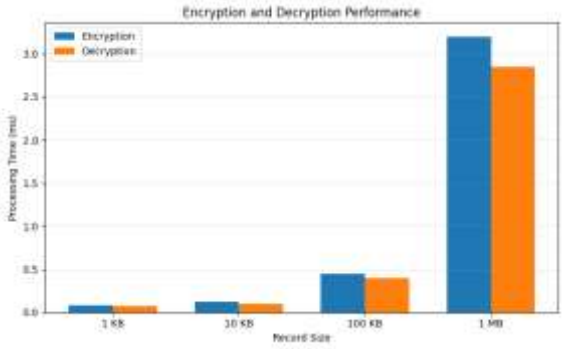


Figure 1: Encryption and Decryption Performance

b. Authentication and Access-Control Evaluation

The authentication and Role-Based Access Control (RBAC) mechanisms are evaluated using valid credentials, invalid login attempts, and requests made by users without sufficient permissions.

Table II. Access-Control Evaluation

Test Case	Requests Tested	Correct Outcome
Authorized login	100	100 granted
Invalid credentials	100	100 denied
Invalid second factor	50	50 denied
Unauthorized record access	100	100 denied
Restricted administrative operation	50	50 denied

The evaluation determines whether the system enforces user permissions correctly. The

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

International Journal of Science, Strategic Management and Technology
Volume **01** Issue **03** December-2025 | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

unauthorized-access denial rate is calculated as the percentage of unauthorized requests successfully rejected.

c. Data Integrity Verification

SHA-256 hashing is used to detect unexpected changes to stored healthcare records by comparing calculated hashes with trusted reference values.

The integrity-detection rate is calculated using the number of modified records detected divided by the total number of modified records tested. Reference hashes must be protected independently to prevent an attacker from changing both the record and its reference value.

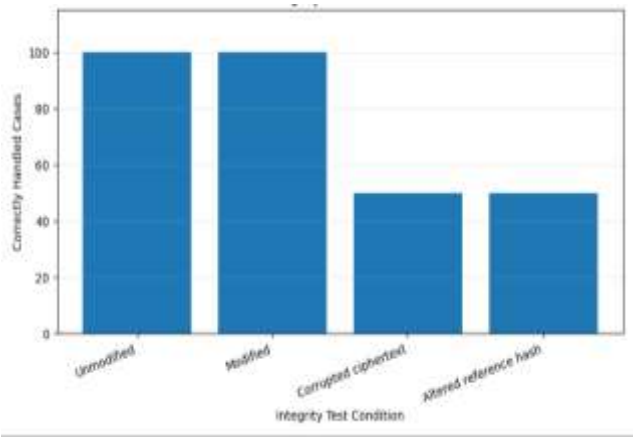


Figure 2: Data Integrity Verification

d. Audit-Log Security Evaluation

The audit-logging mechanism records authentication attempts, access violations, record operations, and other security events. Hash chaining and protected storage can help identify unauthorized alterations.

Table IV. Audit-Log Security Tests

Test Case	Attempts	Detected or Recorded
Successful login events	100	100 recorded
Failed login events	100	100 recorded
Unauthorized access attempts	50	50 recorded
Log modification attempts	50	50 detected
Log deletion attempts	50	50 detected

These tests assess the traceability and tamper-evidence properties of the audit mechanism under the defined experimental conditions.

e. Computational Overhead Analysis

The performance of the secured framework is compared with a baseline system that performs equivalent operations without the additional security controls.

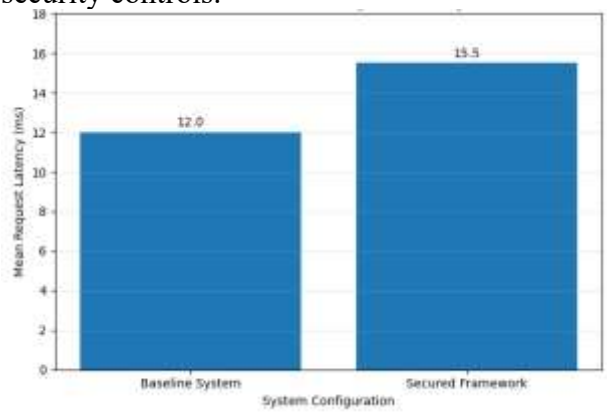


Figure 3: Baseline vs. Secured-System Latency

f. Discussion

The proposed framework integrates encryption, authentication, access control, integrity verification, and audit logging to address multiple healthcare cybersecurity requirements. The experimental results will establish whether each mechanism functions correctly under the defined test conditions and quantify its computational overhead. Comparing the secured framework with a baseline will help determine the performance cost associated with the additional protection.

The final conclusions must be based on verified experimental measurements. The evaluation should also document the threat model, test environment, limitations, and security properties that were not tested. No numerical improvements or claims of comprehensive attack prevention should be reported without supporting evidence.

VII. CONCLUSION

The proposed privacy-preserving healthcare security framework addresses critical challenges associated with protecting Electronic Health Records (EHRs) from unauthorized access, data disclosure, and malicious modification. The framework integrates AES-256-GCM encryption, multi-factor authentication, Role-Based Access Control (RBAC), SHA-256 integrity verification, and tamper-evident audit logging to strengthen healthcare data confidentiality, access security, and accountability. These mechanisms provide complementary layers of protection for sensitive patient information. The framework can be evaluated through controlled security tests and performance measurements to assess access-control effectiveness, integrity-detection capability, audit-log protection, and computational overhead. Its practical effectiveness depends on correct implementation, secure key management,

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

appropriate permission policies, and protection of audit records. Overall, the proposed approach provides a structured foundation for improving electronic health record security while maintaining authorized access to healthcare information. Further experimental validation is required to establish its effectiveness under specific threat conditions.

FUTURE SCOPE

Future work can extend the proposed framework by incorporating advanced threat detection, stronger identity verification, and scalable healthcare data protection mechanisms. Integration with centralized key-management systems or hardware security modules could improve encryption-key protection and lifecycle management. Attribute-Based Access Control (ABAC) could provide more flexible authorization based on user roles, patient consent, and contextual information. Furthermore, integrating a Security Information and Event Management (SIEM) system could support centralized monitoring and correlation of suspicious security events. Future implementations could also evaluate the framework across distributed healthcare environments and cloud-based electronic health record systems. Performance testing with larger datasets, concurrent users, and realistic workloads would provide additional evidence regarding scalability and operational efficiency. Finally, independent security assessments, penetration testing, and compliance-oriented evaluations could help identify vulnerabilities and improve the framework's suitability for practical healthcare deployments.

REFERENCES

[1] F. Ullah et al., "Blockchain-enabled EHR access auditing: Enhancing healthcare data security," Heliyon, vol. 10, no. 16, 2024. https://doi.org/10.1016/j.heliyon.2024.e34407

[2] U. N. Cobrado et al., "Access control solutions in electronic health record systems: A systematic review," Informatics in Medicine Unlocked, vol. 49,2024,Art.no.101552.https://doi.org/10.1016/j.imu.2024.101552

[3] R. Tertulino, N. Antunes, and H. Morais, "Privacy in electronic health records: A systematic mapping study," Journal of Public Health, vol. 32, pp. 435–454, 2024. https://doi.org/10.1007/s10389-022-01795-z

[4] R. Walid, K. P. Joshi, and S. G. Choi, "Comparison of attribute-based encryption schemes in securing healthcare systems," Scientific Reports, vol. 14, Art. no. 7147, 2024. https://doi.org/10.1038/s41598-024-57692-w

[5] E. Psarra et al., "Permissioned blockchain network for proactive access control to electronic health records," BMC Medical Informatics and Decision Making, vol. 24, Art. no. 303, 2024. https://doi.org/10.1186/s12911-024-02708-8

[6] P. Duan et al., "Secure collaborative EHR sharing using multi-authority attribute-based proxy re-encryption in Web 3.0," Computer Networks, vol. 255, Art. no. 110851, 2024. https://doi.org/10.1016/j.comnet.2024.110851

[7] G. Liu et al., "A secure and efficient electronic medical record data sharing scheme based on blockchain and proxy re-encryption," Journal of Cloud Computing, vol. 13, Art. no. 44, 2024. https://doi.org/10.1186/s13677-024-00608-w

[8] "An efficient secure sharing of electronic health records using IoT-based Hyperledger blockchain," International Journal of Intelligent Systems,2024.https://doi.org/10.1155/2024/6995202

[9] "Secure sharing of patient controlled e-health record using an enhanced access control model with encryption based on user identity," International Journal of Advanced Computer Science and Applications, vol. 15, no. 3, 2024. https://doi.org/10.14569/IJACSA.2024.01503124

[10] "Leveraging semantic context to establish access controls for secure cloud-based electronic health records," International Journal of Information Management Data Insights, vol. 4, no. 1, Art. no. 100211, 2024. https://doi.org/10.1016/j.jjimei.2023.100211

[11] "A blockchain-based hybrid encryption technique with anti-quantum signature for securing electronic health records," Complex & Intelligent Systems, vol. 10, pp. 6117–6141, 2024. https://doi.org/10.1007/s40747-024-01477-1

[12] "Design a software reference architecture to enhance privacy and security in electronic health records," IEEE Access, vol. 12, pp. 112157–112179,2024.https://doi.org/10.1109/ACCESS.2024.3441751

[13] "Security and privacy in e-health systems: A review of AI and machine learning techniques," IEEE Access, vol. 12, pp. 148796–148816, 2024. https://doi.org/10.1109/ACCESS.2024.3469215

[14] X. Liang, Y. Liu, and J. Ning, "An access control scheme with privacy-preserving authentication and flexible revocation for smart healthcare," IEEE Journal of Biomedical and

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

Health Informatics, vol. 28, no. 6, pp. 3269–3278, 2024. https://doi.org/10.1109/JBHI.2024.3391218

[15] D. Chen et al., "Flexible and fine-grained access control for EHR in blockchain-assisted e-healthcare systems," IEEE Internet of Things Journal, vol. 11, no. 6, pp. 10992–11007, 2024. https://doi.org/10.1109/JIOT.2023.3328382

[16] K. Vivekrabinson et al., "Secure cloud-based electronic health records: Cross-patient block-level deduplication with blockchain auditing," Journal of Medical Systems, vol. 48, Art. no. 33, 2024. https://doi.org/10.1007/s10916-024-02053-3

[17] S. Kumar and D. K. Shaw, "Efficient access requests management for healthcare data with security and privacy-preserving," Expert Systems with Applications, vol. 267, Art. no. 126194, 2025. https://doi.org/10.1016/j.eswa.2024.126194

[18] D. G. Chakravarthy et al., "Enhancing confidentiality and access control in electronic health record systems using a hybrid hashing blockchain framework," Scientific Reports, vol. 15, Art.no.30379,2025.https://doi.org/10.1038/s41598-025-13831-5

[19] N. Yaqub et al., "Blockchain enabled policy-based access control mechanism to restrict unauthorized access to electronic health records," PeerJ Computer Science, vol. 11, Art. no. e2647, 2025. https://doi.org/10.7717/peerj-cs.2647

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.