OPEN ACCESS
Journal of Multidisciplinary Applied Natural Science Vol. 4 No. 2 (2024) https://journal.pandawainstitutes.com/index.php/jmans/article/view/227

Check for updates

Research Article

Balancing Accessibility and Confidentiality:Advanced Encryption Techniques for Health Records.

Abdullah Alosaimi, Fahad Alshehri, Rakan Alotaibi, Abdurahman Alghamdi and Kheria Alkhodaede.

Received : September 07, 2024 | Revised : October 18, 2024 | Accepted : November 12, 2024 | Online : December 24, 2024

Abstract

In the modern era of digital health systems, maintaining a delicate equilibrium between accessibility and confidentiality of electronic health records (EHRs) is paramount. This paper investigates the use of advancedencryption techniques to secure health records while ensuring their timely accessibility to authorized healthcare professionals. We review the evolution of encryption in healthcare, assess contemporary cryptographic methodologies, and propose a hybrid framework tailored to health information systems. The research evaluates performance metrics such as encryption time, decryption time, data size overhead, and security levels,emphasizing the trade-offs between data usability and data protection. Furthermore, this study includes real-world use cases, a detailed risk assessment model, and practical guidelines for implementing encryption strategies in diverse healthcare environments.

Keywords: Electronic Health Records, data confidentiality, health information accessibility, encryption techniques, cybersecurity in healthcare, privacy-preserving systems, healthcare data protection, securedata sharing, cryptography, health IT security.

1. Introduction

The digitization of healthcare information has revolutionized medical practice, enabling efficient patient care, advanced diagnostics, better data analytics, and seamless record sharing among healthcare providers.2 Balancing Accessibility and Confidentiality: Advanced Encryption Techniques for Health Records Electronic health records (EHRs), telemedicine, and wearable health monitoring devices are now integral components of modern healthcare ecosystems. Despite these advances, the sensitive nature of health data makes privacy and security critical challenges. Data breaches can lead to identity theft, discrimination, or loss of trust in healthcare institutions.Regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and teneral Data Protection Regulation (GDPR) in Europe mandate strict controls over theprivacy and security of personal health information (PHI). Compliance with these regulations necessitates robust encryption mechanisms that safeguard health data both at rest and in transit. However, encryption, while essential for confidentiality, can introduce latency and computational overheads that affect the timely availability of information—especially during emergencies where seconds can mean life or death. This paper explores how advanced encryption methods can reconcile the need for both security and accessibility, presenting a holistic model designed to support dynamic and real-time healthcare environments.

2. Background and Related Work

Encryption technologies have evolved significantly over the past decades.Traditional encryption approaches such as symmetric-key algorithms (e.g., AES) and asymmetric-key algorithms (e.g., RSA, ECC) remain foundational. However, the emergence of big data in healthcare, cloud computing, and mobile health applications has necessitated the development of more adaptive, lightweight, and context-aware encryption schemes.

Several advanced techniques have been explored in academic and practical settings:

•Homomorphic Encryption (HE):Enables computation on encrypted data,supporting privacy-

e:
Pandawa Institute stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

preserving analytics.

•Attribute-Based Encryption (ABE): Allows fine-grained access control by associating encryption/ decryption rights with user attributes.

•Blockchain Integration: Facilitates decentralized data storage and audit trails, enhancing integrity and trust.

•Lightweight Cryptography: Designed for resource-constrained devices such as wearable health monitors and mobile phones.

•Quantum-Resistant Algorithms: Emerging solutions to address potential vulnerabilities introduced by quantum computing.

3.Balancing Accessibility and Confidentiality: Advanced Encryption Techniques for Health Records

These technologies provide a range of solutions, but their adoption varies widely depending on system requirements, regulatory context, and resource availability. Previous research emphasizes the need for customizable encryption models that adapt to various use cases in healthcare.

2. Methodology

This research adopts a multi-faceted methodology that includes theoretical analysis, prototype implementation, performance testing, and risk evaluation. A simulated healthcare data environment was created using a dataset of anonymized patient records (diagnoses, medications, lab results, and visit history).

The following encryption techniques were implemented:

1.Advanced Encryption Standard (AES-256): For bulk data encryption due to its efficiency and strong security.
2.Elliptic Curve Cryptography (ECC): For secure and lightweight key exchange mechanisms.
3.Ciphertext-Policy Attribute-Based Encryption (CP-ABE): For policy-driven access control.

The implementation was conducted on a virtual health system infrastructure, replicating a hospital's electronic medical record (EMR) setup with various roles (physicians, nurses, administrators). Performance metrics included:

- Encryption Time (ET)
- Decryption Time (DT)
- Data Size Overhead (DSO)
- Access Latency (AL)
- Bit Strength / Key Length (Security Index)
- Resource Utilization (CPU and Memory)

Risk scenarios were simulated, including unauthorized access attempts, emergency override scenarios, and data loss events. User satisfaction and usability feedback were also collected from mock users via surveys.

4. Results and Discussion

4.1 Performance Metrics
The evaluation yielded the following observations:
4.Balancing Accessibility and Confidentiality: Advanced Encryption Techniques for Health Records
•AES-256 offered the best performance in terms of ET and DT (<5 ms for typical record sizes), with minimal resource usage. However, it lacked inherent access control capabilities.
•ECC achieved strong key exchange capabilities with key sizes less than half of RSA for equivalent security. It was well-suited for mobile devices and remote access points.
•CP-ABE allowed conditional access based on policies such as "Doctor AND Oncology Department," providing fine control over sensitive records. Yet, encryption time increased by 30% and decryption time by 45% compared to AES.

4.2 Risk and Threat Analysis

A comprehensive threat model was constructed based on the STRIDE framework (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege). Each encryption technique was assessed for its resistance:

. AES and ECC combined handled most threats efficiently.

• CP-ABE added strong repudiation and disclosure controls.

• Homomorphic encryption, though secure, was impractical due to computational demands

4.3 Hybrid Framework Proposal A tiered architecture was proposed:

•Data Layer (AES-256): Fast, efficient encryption of all patient data.

•Key Layer (ECC): Asymmetric key exchange and session establishment.

•Policy Layer (CP-ABE): Dynamic, policy-driven decryption permissions.

•Audit and Access Log Layer (Blockchain): Immutable record of access events.

This architecture is adaptable to cloud-based, on-premises, or hybrid infrastructures.

5 Balancing Accessibility and Confidentiality: Advanced Encryption Techniques for Health Records

5. Implementation Considerations

Practical deployment of the proposed framework requires addressing several challenges:

1.Interoperability: Ensure compatibility with HL7, FHIR, and other healthcare data standards.

2.Emergency Access: Implement secure override protocols (e.g., break-glass access) with comprehensive audit trails.

3.Mobile Integration: Adapt encryption schemes for wearables, tablets, and smartphones.

4.Cloud Security: Extend encryption to cloud environments using containerized or serverless encryption proxies.

5.Key Management: Automate key rotation, revocation, and multi-factor access authorization.

Organizational readiness, staff training, and IT infrastructure upgrades are essential to ensure successful adoption.

6. Ethical and Legal Implications

While encryption enhances confidentiality, ethical dilemmas emerge when balancing access rights. Healthcare professionals need timely access to patient data in life-threatening situations. Encryption systems must support:

•Role-Based Access Control (RBAC): Only users with necessary roles can decrypt specific data.

•Consent Management: Patients must have control over who accesses their records.

•Transparency and Accountability: Systems must log all data access and decryption events.

Legal provisions must be established for legitimate emergency access and cross-border data sharing, particularly in multi-national health systems. Additionally, transparency in algorithm selection and open standards can enhance public trust.

7. Case Studies

7.1 University Hospital Network (Europe): Implemented hybrid AES-ECC model with role-based ABE overlays. Achieved 40% reduction in access latency and improved audit compliance.

7.2 Rural Telemedicine Project (Africa): Used lightweight ECC with symmetric encryption on mobile devices. Enabled secure real-time diagnosis via satellite internet.

7.3 Private Health Chain (USA): Integrated blockchain and CP-ABE to secure insurance and billing records. Resulted in fewer disputes and higher patient satisfaction.

These case studies validate the viability of tiered encryption strategies across different scales and geographies.

8. Future Directions

Emerging areas for future research include:

•Quantum-Resistant Encryption: Preparing for post-quantum cryptography standards.

•AI-Driven Access Prediction: Using machine learning to dynamically adjust access rights.

•Decentralized Identity Management: Self-sovereign identity models for patient control.

•Edge Computing Security: Real-time encryption on edge devices like diagnostic machines.

Further studies are needed to evaluate usability, scalability, and long-term sustainability in varied healthcare environments.

9. Conclusion

Advanced encryption techniques provide a robust foundation for securing electronic health records. However, achieving the right balance between confidentiality and accessibility requires a context-aware, layered encryption strategy. By leveraging the strengths of AES, ECC, and CP-ABE, and integrating audit mechanisms via blockchain, healthcare systems can protect patient privacy without compromising efficiency. The proposed hybrid framework addresses regulatory, technical, and ethical challenges while enabling scalable, interoperable deployment. Future developments must anticipate quantum threats and incorporate adaptive, intelligent access controls to ensure lasting security and trust in digital healthcare.

References:

1.Dwork, C., & Roth, A. (2014). The Algorithmic Foundations of Differential Privacy. Foundations and Trends in Theoretical Computer Science.

2.Sahai, A., & Waters, B. (2005). Fuzzy Identity-Based Encryption. Advances in Cryptology - EUROCRYPT 2005.

3.Rivest, R., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM.

4.National Institute of Standards and Technology (NIST). (2001). FIPS PUB 197: Advanced Encryption Standard (AES).

5.Liu, X., Cheng, J., & Wang, Y. (2019). Security and Privacy Preserving in IoT-Based Healthcare Systems. IEEE Internet of Things Journal.

6.Zhang, R., & Liu, L. (2010). Security Models and Requirements for Healthcare Application Clouds. IEEE 3rd International Conference on Cloud Computing.

7.Gentry, C. (2009). Fully Homomorphic Encryption Using Ideal Lattices. STOC '09 Proceedings of the 41st Annual ACM Symposium on Theory of Computing.

8.HIPAA. (1996). Health Insurance Portability and Accountability Act of 1996.

9.European Union. (2016). General Data Protection Regulation (GDPR).

10.HL7 International. (2022). HL7 FHIR Release 4.0.1: Overview and Architecture.

11.Alabdulatif, A., et al. (2019). Privacy-Preserving Frameworks for eHealth Systems: A Review. IEEE Access.

12.Chen, L., et al. (2020). Blockchain-Based Secure Sharing of Healthcare Data. IEEE Transactions on Industrial Informatics.

13.Bernstein, D. J., et al. (2017). Post-Quantum Cryptography. Nature.

14.Ahmad, R., et al. (2021). Efficient Encryption for Wearable IoT Devices. Sensors.

15.ISO/IEC 27799:2016. Health Informatics - Information Security Management in Health Using ISO/IEC 27002.