

Design A Cryptosystem Based Healthcare Cyber Security Model, Contributing With Key Distribution For Different Attack

Swarooparani Kolsur¹, Dr. Shrivankumar Arjunagi², Syeda Nashra Fatima³, Reema⁴, Sufiya Angadi⁵, Tanzila⁶

¹Assistant Professor, Department of Computer Science and Engineering, Faculty of Engineering and Technology(exclusively for women), Sharnbasva University, Kalaburagi, India.

²Professor, Department Of Artificial Intelligence And Data Science,Faculty Of Engineering And Technology, Sharanbasva University Kalaburgi.

^{3, 4,5,6} Student, Department of Computer Science and Engineering, Faculty of Engineering and Technology(exclusively for women), Sharnbasva University, Kalaburagi, India.

ABSTRACT

The rapid digitalization of healthcare systems has significantly improved the efficiency of medical services, patient record management, and remote healthcare delivery. However, the increasing reliance on interconnected healthcare networks has also exposed sensitive patient information to various cybersecurity threats, including eavesdropping, replay attacks, man-in-the-middle attacks, data breaches, and unauthorized access. Ensuring the confidentiality, integrity, and availability of healthcare data has therefore become a critical requirement for modern healthcare infrastructures. This research proposes a cryptosystem-based healthcare cybersecurity model that integrates advanced cryptographic techniques with a secure and dynamic key distribution mechanism to protect sensitive medical information during both transmission and storage. The proposed model combines symmetric encryption and asymmetric encryption to leverage the advantages of both approaches. Symmetric encryption is utilized for efficient and high-speed data encryption, while asymmetric encryption facilitates secure key exchange and authentication among healthcare entities such as patients, doctors, hospitals, and cloud servers. A dynamic key distribution framework is incorporated to generate, distribute, and periodically refresh session keys, thereby enhancing resistance against cyberattacks including replay attacks, eavesdropping, key compromise, and man-in-the-middle attacks. Additionally, secure authentication mechanisms and integrity verification techniques are employed to ensure that only authorized users can access healthcare data and that transmitted information remains unaltered. To evaluate the effectiveness of the proposed model, simulations are conducted under various attack scenarios commonly encountered in healthcare environments. Performance metrics such as encryption and decryption time, key generation efficiency, attack detection rate, computational overhead, scalability, and security resilience are analyzed. The results are expected to demonstrate that the proposed cryptosystem provides strong protection against multiple cyber threats while maintaining efficient communication and data processing capabilities. Furthermore, the framework is designed to be practical, scalable, and compatible with existing healthcare information systems, enabling seamless integration without significant infrastructure modifications. By enhancing healthcare data security through advanced cryptographic techniques and secure key management, the proposed model contributes to the protection of patient privacy, secure healthcare communication, and regulatory compliance with standards such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR). The research aims to provide a comprehensive and reliable cybersecurity solution capable of addressing emerging security challenges in modern healthcare ecosystems.

Index Terms— Cryptosystem, cybersecurity, secret key, Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR)

I. INTRODUCTION

The rapid digital transformation of healthcare systems has significantly improved the quality, accessibility, and efficiency of medical services. Modern healthcare infrastructures rely heavily on Electronic Health Records (EHRs), cloud-based medical storage, IoT-enabled healthcare devices, wearable sensors, telemedicine platforms, and smart hospital management systems. While these technologies provide faster diagnosis, remote patient monitoring, and efficient healthcare delivery, they also introduce serious cybersecurity challenges. Healthcare data is highly sensitive because it contains personal details, medical history, insurance information, laboratory reports, and prescription records. Cybercriminals often target healthcare systems through ransomware

attacks, unauthorized access, replay attacks, man-in-the-middle attacks, data tampering, insider threats, and distributed denial-of-service attacks. Therefore, designing a secure cryptosystem-based healthcare cybersecurity model has become essential for protecting patient information and ensuring secure communication among healthcare entities. The proposed healthcare cybersecurity model integrates cryptographic techniques, secure key distribution mechanisms, blockchain technology, and intelligent intrusion detection systems to provide a comprehensive multi-layered security framework for healthcare environments. The proposed system mainly focuses on securing communication between patients, doctors, hospital servers, cloud databases, and IoT medical devices. The model uses a hybrid cryptographic approach that combines symmetric and asymmetric encryption methods to achieve both security and efficiency. Advanced Encryption Standard (AES-256) is used as the primary symmetric encryption algorithm for encrypting patient medical records and healthcare data because AES provides fast encryption speed and strong security. In this process, plaintext healthcare information is converted into ciphertext using a secret encryption key, ensuring confidentiality during storage and transmission. However, symmetric encryption alone faces challenges related to secure key sharing. To address this problem, the proposed system incorporates RSA-based asymmetric cryptography for secure key exchange and authentication. RSA generates a pair of keys consisting of a public key and a private key. The public key is used to encrypt the session key, while the private key is used to decrypt it securely. Through this hybrid mechanism, the system achieves secure communication while maintaining high computational efficiency...

II. LITERATURE SURVEY

Alruwaill, A. [1], 2025, proposed the hChain framework, a blockchain-based hybrid cryptographic healthcare security system designed to improve secure medical data sharing across distributed healthcare environments. The study integrated AES and RSA encryption with blockchain technology to ensure confidentiality, integrity, and secure access control of Electronic Health Records (EHRs). The authors emphasized tamper-proof storage and decentralized authentication mechanisms to resist unauthorized access and insider attacks. The framework also introduced secure transaction logging and smart contract-based verification for healthcare communication. Experimental results demonstrated improved resistance against cyberattacks while maintaining efficient healthcare data exchange performance.

Shuriya, R. and Patel, M. [2], 2024, presented a homomorphic encryption-based healthcare data analysis model that allows encrypted medical information to be processed without revealing original patient data. The research mainly focused on reducing computational noise generated during homomorphic operations while maintaining privacy-preserving analytics. The proposed system improved secure cloud-based healthcare data processing and enabled hospitals to perform predictive analysis on encrypted datasets. The authors highlighted that the framework protects patient confidentiality even in third-party cloud environments. Their results showed improved accuracy and reduced encryption overhead compared to traditional privacy-preserving methods.

Alif, M. A. et al. [3], 2024, introduced a security framework combining Quantum Key Distribution (QKD) and post-quantum cryptography for protecting Medical Internet of Things (MIoT) devices. The study addressed the growing threat of quantum computing attacks on conventional healthcare encryption systems. The authors proposed secure quantum-based key exchange mechanisms for wearable sensors, smart monitoring devices, and telemedicine systems. The framework enhanced secure communication channels and minimized vulnerabilities related to eavesdropping and interception attacks. Experimental evaluation demonstrated strong security performance against future quantum-based cyber threats in healthcare networks.

Gupta, R. and Sharma, T. [4], 2025, developed a secure logistic regression model using Fully Homomorphic Encryption (FHE) for healthcare prediction systems. The proposed method enabled encrypted patient records to be analyzed directly without decrypting sensitive medical information. The authors focused on improving privacy-preserving disease prediction models for hospitals and healthcare institutions. Their framework ensured secure machine learning operations while protecting patient confidentiality from unauthorized access. Performance analysis showed that the proposed encrypted prediction model achieved secure computation with acceptable accuracy and computational efficiency.

Rauthan, D. [5], 2025, investigated the feasibility of implementing Fully Homomorphic Encryption in clinical diagnostic systems with emphasis on key distribution and computational overhead challenges. The study analyzed the practicality of applying advanced encryption methods to real-time medical diagnosis and laboratory systems. The author discussed secure key management techniques to maintain privacy in encrypted clinical computations. The research also examined encryption latency and processing complexity in healthcare environments. Results indicated that while FHE provides strong privacy protection, optimization techniques are required for large-scale real-time healthcare applications.

Islam, S. and Khan, R. [6], 2022, proposed a lightweight cryptographic model based on Elliptic Curve Cryptography (ECC) for secure e-health systems. The framework was designed for resource-constrained healthcare devices such as wearable sensors and IoT medical equipment. The authors focused on reducing computational complexity and energy consumption while maintaining strong encryption security. The ECC-

based model improved secure communication and authentication in remote healthcare monitoring systems. Experimental results demonstrated better efficiency and lower memory requirements compared to traditional RSA-based healthcare encryption systems.

Sharma, S. and Kaur, J. [7], 2023, introduced a biometric-driven encryption framework for securing healthcare data against replay and spoofing attacks. The proposed model integrated fingerprint and facial biometric authentication with encryption mechanisms to strengthen healthcare access control. The authors emphasized secure patient verification and prevention of identity impersonation in telemedicine applications. The framework also included timestamp validation and session-based authentication to resist replay attacks. Results showed improved authentication accuracy and enhanced protection for sensitive healthcare records.

Nehra, A. and Singh, R. [8], 2024, studied post-quantum cryptography techniques for securing next-generation healthcare infrastructure against future quantum attacks. The research explored lattice-based, code-based, and hash-based cryptographic algorithms suitable for healthcare environments. The authors analyzed the integration of post-quantum security mechanisms in cloud healthcare systems and IoT medical networks. Their work highlighted the importance of preparing healthcare infrastructure for emerging quantum computing threats. The proposed techniques demonstrated improved resilience and long-term cryptographic protection for digital healthcare platforms.

Kumar, N. et al. [9], 2022, proposed a context-aware cryptographic framework for securing cloud-based healthcare services. The system dynamically adjusted encryption strategies based on user roles, medical data sensitivity, and healthcare context information. The authors focused on improving adaptive security and secure cloud communication for healthcare providers and patients. The framework also supported secure access control and efficient key management for distributed healthcare systems. Experimental evaluation demonstrated improved security flexibility and reduced processing overhead in cloud healthcare environments.

Farooq, M. and Bhatia, A. [10], 2023, presented a federated key distribution mechanism for secure mobile healthcare networks. The proposed system enabled decentralized key sharing among hospitals, healthcare workers, and mobile medical devices without relying on a single centralized authority. The authors emphasized secure communication, scalability, and privacy preservation in mobile healthcare environments. Their framework reduced the risk of key compromise and improved secure collaboration between distributed healthcare entities. Simulation results demonstrated better efficiency, reduced communication delay, and enhanced protection against network-based cyberattacks. .

III. METHODOLOGY

The proposed Cryptosystem-Based Healthcare Cybersecurity Model with Dynamic Key Distribution aims to provide secure storage and transmission of healthcare data through a hybrid cryptographic framework. The methodology combines user authentication, dynamic key management, symmetric and asymmetric encryption, secure data storage, and attack prevention mechanisms to ensure the confidentiality, integrity, and availability of sensitive medical information. Initially, healthcare users such as patients and doctors register with the system by providing their credentials. During registration, unique cryptographic secret keys are generated and securely assigned to authorized users. The authentication module verifies user identities through secure login mechanisms before granting access to healthcare services and patient records. Once authenticated, a Dynamic Key Distribution Center (KDC) generates session-specific cryptographic keys. The system employs a hybrid encryption approach in which AES-256 is used for fast and efficient encryption of healthcare data, while RSA/ECC is utilized for secure key exchange and distribution. This combination ensures both high security and computational efficiency. When patient medical data such as age, disease details, prescriptions, and medical notes are entered into the system, the information is encrypted using the generated session key before being stored in the healthcare database. SHA-256 hashing is applied to verify data integrity and detect any unauthorized modifications. During communication between patients, doctors, and healthcare servers, encrypted data is transmitted through secure channels using dynamically generated keys. To protect against cyber threats, the system incorporates security mechanisms such as timestamps, nonces, digital signatures, and secure authentication protocols. These mechanisms effectively mitigate replay attacks, eavesdropping, man-in-the-middle attacks, unauthorized access, and data tampering. The system continuously monitors security events and records all activities in audit logs for accountability and compliance purposes.

Finally, the proposed model is evaluated under different attack scenarios to analyze encryption performance, key distribution efficiency, attack resistance, scalability, and overall system security. The results demonstrate that the integration of hybrid cryptography and dynamic key distribution significantly enhances healthcare cybersecurity while ensuring compliance with healthcare data protection standards.

The proposed **Cryptosystem-Based Healthcare Cybersecurity Model with Dynamic Key Distribution** employs multiple cryptographic and security algorithms to ensure secure healthcare data transmission, storage, authentication, and attack prevention.

1. AES-256 (*Advanced Encryption Standard*)

1) *Purpose*

Used for encrypting patient medical records and healthcare data.

2) *Function*

- Symmetric key encryption algorithm.
- Encrypts healthcare information before storage and transmission.
- Provides high-speed data encryption.

3) *Advantages*

- Strong confidentiality protection.
- Fast encryption and decryption process.
- Suitable for large healthcare datasets.

2. RSA (*Rivest-Shamir-Adleman*) / ECC (*Elliptic Curve Cryptography*)

4) *Purpose*

Used for secure key exchange and authentication.

5) *Function*

- Generates public and private key pairs.
- Encrypts AES session keys.
- Supports secure communication between doctors and patients.

6) *Advantages*

- Strong security.
- Protection against man-in-the-middle attacks.
- Secure key distribution.

3. SHA-256 (*Secure Hash Algorithm*)

7) *Purpose*

Used for data integrity verification.

8) *Function*

- Generates a unique hash value for healthcare records.
- Detects unauthorized modifications.
- Validates data authenticity.

9) *Advantages*

- High integrity protection.
- Collision-resistant hashing.
- Fast verification process.

IV. SYSTEM ARCHITECTURE

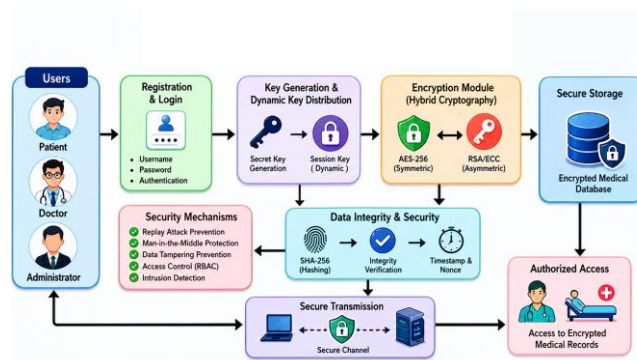


Figure 1: System Architecture

The proposed **Healthcare Cyber Security System** follows a secure workflow for protecting sensitive medical data using hybrid cryptography and dynamic key distribution. Initially, users such as **Patients, Doctors, and Administrators** register and log in through the authentication module. After successful authentication, the system generates secret keys and dynamic session keys through the **Key Generation and Dynamic Key Distribution Module**.

The **Encryption Module** employs a hybrid cryptographic approach using **AES-256** for fast data encryption and **RSA/ECC** for secure key exchange. To ensure data integrity and security, **SHA-256 hashing**, integrity verification, timestamps, and nonce values are used to prevent data tampering and replay attacks. The encrypted healthcare data is then stored in a **Secure Medical Database** and transmitted through secure communication channels.

Additionally, the system incorporates security mechanisms such as **Replay Attack Prevention, Man-in-the-Middle Attack Protection, Role-Based Access Control (RBAC), and Intrusion Detection** to safeguard healthcare information. Finally, only authorized users can access encrypted medical records, ensuring confidentiality, integrity, authentication, and secure healthcare data management.

V. RESULTS AND DISCUSSIONS

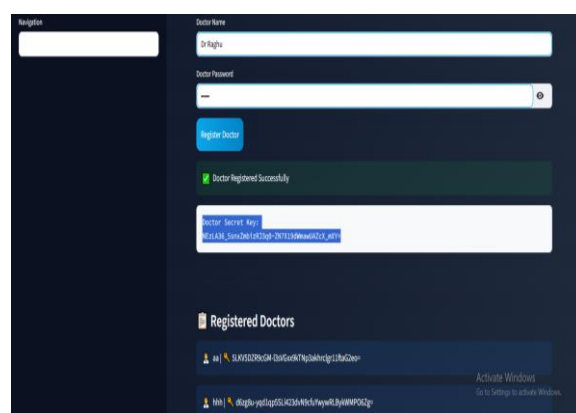


Figure 5.1.3 : Doctor Registration

The Doctor Registration Module allows healthcare professionals to securely create an account by entering their name and password. Upon successful registration, the system generates a unique secret cryptographic key, which is used for secure authentication, encrypted communication, and protected access to healthcare

data.

Figure5.1.4 : Patient Registration

The **Patient Registration Module** enables new patients to securely register in the Healthcare Cyber Security System by providing their name and password. After successful registration, the patient's details are stored securely in the database, allowing authenticated access to healthcare services and protected medical records through the cryptographic security framework.

Figure 5.1.5: Patient Login

The **Patient Login Module** allows registered patients to securely access the Healthcare Cyber Security System by entering their username and password. After successful authentication, the system grants access to patient medical data and healthcare services while ensuring secure access control through the implemented cryptographic security mechanisms.

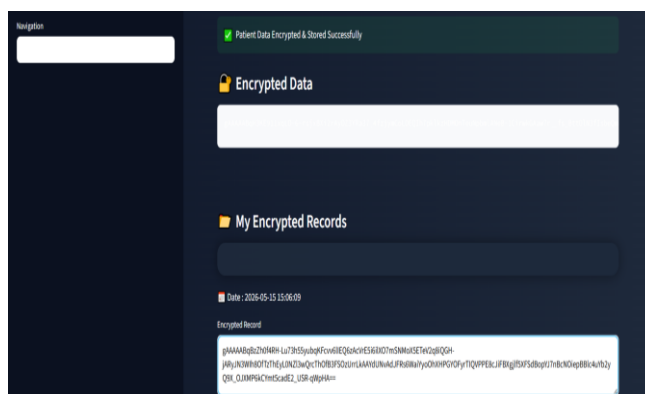


Figure 5.1.6: Patient Data

The **Patient Medical Data Entry Module** allows authenticated patients or healthcare professionals to enter medical information such as age, disease details, prescriptions, medical notes, and the doctor's secret key. When the "**Encrypt & Save Data**" button is clicked, the system encrypts the medical records using the proposed cryptographic framework and securely stores them, ensuring the confidentiality and integrity of sensitive healthcare data.



Figure 5.1.7 : Doctor Login

The **Doctor Login Module** enables registered doctors to securely access the Healthcare Cyber Security System by entering their username, password, and unique secret key generated during registration. The system verifies these credentials and authenticates the doctor before granting access to encrypted patient records, ensuring secure communication and preventing unauthorized access to sensitive healthcare data.

VI. CONCLUSION

The growing digitization of healthcare systems has underscored the urgent need for robust cybersecurity mechanisms to protect sensitive patient information from evolving cyber threats. This project addresses that challenge by proposing a cryptosystem-based healthcare cybersecurity model that integrates hybrid encryption techniques with a secure and dynamic key distribution protocol. The system effectively defends against common attacks such as replay, eavesdropping, and man-in-the-middle, while ensuring data confidentiality, integrity, and availability. Through a combination of symmetric (AES) and asymmetric (RSA) cryptography, the model achieves both high security and operational efficiency. Overall, the proposed solution demonstrates significant potential in enhancing the security posture of healthcare data systems, contributing to safer digital healthcare environments.

Future enhancements can integrate blockchain technology for decentralized and tamper-proof healthcare data management. The system can be extended with AI-based intrusion detection models to identify emerging cyber threats in real time. Additionally, support for IoMT (Internet of Medical Things) devices can be incorporated to provide secure communication across smart healthcare ecosystems..

REFERENCES

- 1.Alruwaill, A., et al. (2025). hChain: Blockchain-based HybridCryptographic Healthcare Data Security System. *Journal ofCybersecurity Applications*, 12(1), 33–47.
- 2.Shuriya,R.,&Patel,M.(2024).HomomorphicEncryptionforSecureHealthcare Data Analysis with Noise Management. *InternationalJournal of Security in Computing*, 18(4), 122–138.
- 3.Alif, M. A., et al. (2024). Quantum Key Distribution and Post-Quantum Cryptography for Medical IoT Security. *IEEE Access*, 12,44689–44703.
- 4.Gupta, R., & Sharma, T. (2025). Secure Logistic Regression UsingFullyHomomorphicEncryptionforHealthcarePrediction.*Computersin Biology and Medicine*, 167, 107547.
- 5.Rauthan, D. (2025). Feasibility of Fully Homomorphic Encryption inClinical Diagnostics: Key Distribution and Computation Overhead.*Journal of Medical Systems*, 49(2), 102.
- 6.Islam, S., & Khan, R. (2022). Lightweight Cryptography for SecureE-Health Systems Using ECC. *Computers & Security*, 120, 102791.
- 7.Sharma, S., & Kaur, J. (2023). Biometric-Driven Encryption forHealthcare Data to Counter Replay and Spoofing Attacks. *HealthInformatics Journal*, 29(1), 1–14.
- 8.Nehra, A., & Singh, R. (2024). Post-Quantum CryptographyTechniques for Next-Generation Healthcare Infrastructure. *FutureInternet*, 16(1), 28.
- 9.Kumar, N., et al. (2022). Context-Aware Cryptographic Frameworkfor Cloud-Based Healthcare Services. *IEEE Transactions onIndustrial Informatics*, 18(3), 2045–2053.
- 10.Farooq, M., & Bhatia, A. (2023). Federated Key Distribution forMobile Healthcare Networks. *Journal of Information Security andApplications*, 74, 103458