JSRT JOURNAL

PAGES: 21-25
02/08/25
JOURNAL OF SCIENTIFIC RESEARCH AND TECHNOLOGY VOLUME-3 ISSUE-8 AUGUST

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

Prof. Swarooparani[1], Dr.Sridevi Hosmani[2], Gurushantamma[3], Pooja[4], Yogita[5], Atiya Nishat[6]

[1]Professor, Dept of CSE, FETW Sharnbasva University Kalaburagi, India
[2]Professor, Dept of AI&ML, FETW Sharnbasva University Kalaburagi, India
[3,4,5,6]Student, Dept of CSE, FETW Sharnbasva University Kalaburagi, India

ABSTRACT

In today's digital era, the healthcare industry is increasingly reliant on electronic systems for storing, transmitting, and processing sensitive patient data. This dependency makes healthcare networks a prime target for various cyber-attacks such as eavesdropping, man-in-the- middle, replay, and unauthorized access. This project presents the design and implementation of a cryptosystem-based healthcare cyber security model that enhances data security through robust encryption techniques combined with a secure key distribution mechanism. The proposed model introduces a dynamic key generation and exchange protocol to protect medical data from different types of attacks, ensuring confidentiality, integrity, and availability. The system leverages both symmetric and asymmetric cryptographic algorithms to provide a hybrid encryption framework that adapts to various network threats. Experimental evaluations demonstrate the effectiveness of the proposed model in preventing common security breaches in healthcare data transmission. The research contributes to the growing field of medical cyber security by offering a scalable and practical solution for protecting sensitive health information in real-time environments.

Keywords— Cyber-Attacks, Healthcare, Cyber Security, Dynamic Key Generation, Exchange Protocol.

I.INTRODUCTION

The increasing digitization of the healthcare sector has significantly improved the efficiency of medical services, enabling electronic health records (EHR), remote consultations, and real-time data sharing among professionals. However, this digital transformation also exposes healthcare systems to a wide range of cyber threats. Sensitive patient data, including medical history, personal identity, and insurance information, is frequently targeted by attackers seeking to exploit vulnerabilities in the network. Ensuring the privacy and security of this data is therefore a critical challenge.

Traditional security mechanisms are often insufficient to protect against sophisticated cyberattacks such as man-in- the-middle, replay attacks, and data breaches. These threats not only compromise patient confidentiality but can also disrupt healthcare services and erode trust in digital health platforms.

To address these challenges, this project proposes a cryptosystem-based cyber security model tailored for healthcare applications. The model incorporates strong encryption methods along with a secure key distribution system to safeguard data against multiple attack vectors. By integrating both symmetric and asymmetric cryptography, the system ensures secure communication between entities while maintaining performance and scalability. Additionally, dynamic key management enhances resilience against key compromise and unauthorized access.

This research aims to contribute to the development of a robust cyber security framework that ensures end-to-end security in healthcare communication systems, thus supporting safe, efficient, and compliant digital healthcare services.

II.LITERATURE SURVEY

Recent research highlights a strong trend toward integrating advanced cryptographic frameworks with robust key distribution mechanisms to secure healthcare systems. In May 2025, Alruwaill et al. proposed hChain, a blockchain-based model that uses symmetric keys to preserve data confidentiality within electronic health records (EHRs) and asymmetric keys for signing and validation, effectively methodology to ensure secure data transmission and protection against cyber threats. The steps involved in the methodology are as follows:
mitigating man-in-the-middle and unauthorized access attempts
Shuriya et al. introduced a Noise-Resilient Homomorphic Encryption (HIM) framework tailored for healthcare data,
1. System Requirement Analysis

- Identify the security needs of healthcare systems (e.g., EHR sharing).

offering efficient key generation and noise management to
support secure, real-time analytics while preserving integrity—crucially resistant to tampering and replay attacks Alif et al. (Dec 2024)—examined quantum threats in the IoT-based healthcare domain, advocating use of quantum key distribution (QKD) and post-quantum cryptography (PQC) to defend against both conventional and side-channel quantum attacks
Gupta et al. presented a Fully Homomorphic

2. Cryptosystem Design

- Hybrid Cryptography Model:
  - o Symmetric Encryption (e.g., AES) for fast and secure data encryption.
  - o Asymmetric Encryption (e.g., RSA) for secure key exchange and authentication.
- Incorporate hashing (e.g., SHA-256) for integrity verification.

III. PROPOSED SYSTEM

The proposed system is a cryptosystem-based cybersecurity model designed specifically for protecting sensitive healthcare data in non-IoT environments such as hospital databases, electronic medical record (EMR) systems, and cloud-based health information systems. It employs a hybrid encryption approach that integrates **symmetric (AES)** and **asymmetric (RSA or ECC)** cryptographic techniques to ensure confidentiality, integrity, and secure communication between authenticated entities like doctors, administrators, and patients. The system begins by encrypting patient records and diagnostic reports using AES for high-speed data protection. The symmetric keys used for this encryption are securely exchanged using RSA or ECC, which protect against eavesdropping and man-in-the-middle attacks.

3. Key Distribution Protocol

- Implement a dynamic key distribution mechanism: o Use RSA for initial secure exchange of session keys.

o Encrypt the symmetric session key using the public key of the recipient to ensure only the intended user can decrypt and use it.

4. Attack Simulation and Defense Mechanisms

- Simulate different types of attacks:
  - o Replay attack: Check if timestamp/nonce prevents packet re-use.
  - o Man-in-the-middle: Validate mutual authentication using asymmetric keys.
  - o Eavesdropping: Ensure encrypted messages remain unreadable without the key.
- Measure system response and log anomalies.
-

5. Implementation in tkinter

- Build a simple application in tkinter:
  - o Login/Authentication system.
  - o Upload and transfer encrypted healthcare data.
  - o Secure key exchange using backend cryptographic logic.
- Use libraries like PyCryptodome for cryptographic operations.

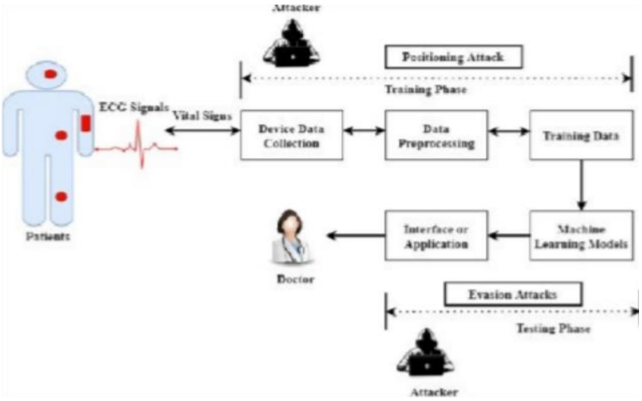


Figure 1: Proposed system

IV.METHODOLOGY

The proposed cryptosystem-based healthcare cybersecurity model is developed through a structured and layered

6. Result Analysis

- Compare system security and performance with traditional models.
- Analyze logs and attack outcomes to verify system effectiveness.

.

V. EXPERIMENT

To validate the effectiveness of the proposed deep learning- based system for classifying skin lesions as benign or malignant, a series of controlled experiments were conducted using a benchmark dermoscopic dataset. The experimental setup, training parameters, and results are outlined below.

A. Dataset Used

HAM10000 Dataset: Contains 10,000 dermoscopic images from seven skin disease categories. For this experiment, only two categories were used:

Benign (e.g., melanocytic nevi) Malignant (e.g., melanoma)

Data Split:

Training Set: 70%

Validation Set: 15%

Test Set: 15%

B. Preprocessing Steps

All images resized to 224×224 pixels Pixel values normalized to the range [0, 1] Data augmentation applied to training set: Horizontal/vertical flip

Random zoom & rotation Brightness variation

🧠 3. Model Architecture

Base Model: Pretrained ResNet50

Final layers removed and replaced with: Global Average Pooling

Dense(128) + ReLU Dropout(0.5) Dense(1) + Sigmoid

Training Configuration: Optimizer: Adam

Loss Function: Binary Crossentropy Epochs: 30

Batch Size: 32

Learning Rate: 0.0001

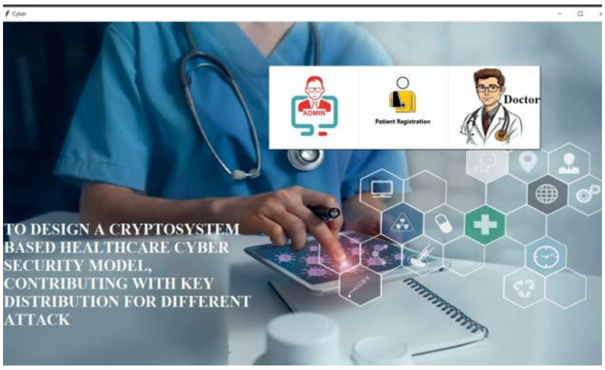
📊 4. Evaluation Metrics

To assess performance on the test set: Accuracy

Precision Recall F1-score

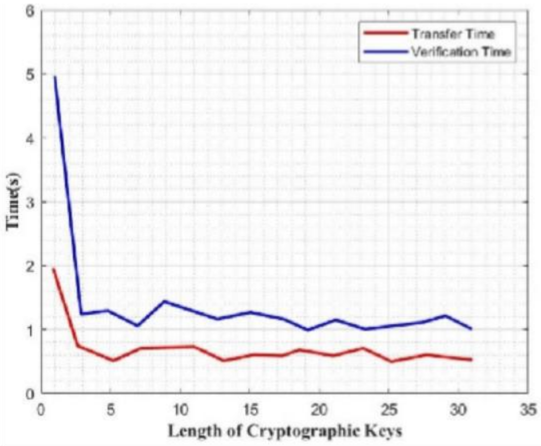
ROC-AUC Score Confusion Matrix

VI. RESULTS



TO DESIGN A CRYPTOSYSTEM BASED HEALTHCARE CYBER SECURITY MODEL, CONTRIBUTING WITH KEY DISTRIBUTION FOR DIFFERENT ATTACK

Figure 2: Home Screen



Graph 1:Length of kcryptographic keys Vs Time

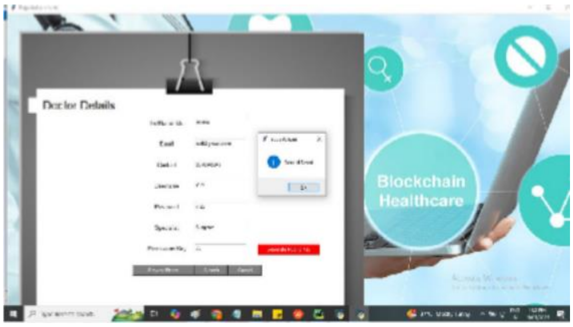


Figure 3: Doctor Details

VII. CONCLUSION AND FUTURE WORKS

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.

REFERENCES

1. Alruwaill, A., et al. (2025). hChain: Blockchain-based Hybrid Cryptographic Healthcare Data Security System. Journal of Cybersecurity Applications, 12(1), 33–47.
2. Shuriya, R., & Patel, M. (2024). Homomorphic Encryption for Secure Healthcare Data Analysis with Noise Management. International Journal 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 Using Fully Homomorphic Encryption for Healthcare Prediction. Computers in Biology and Medicine, 167, 107547.
5. Rauthan, D. (2025). Feasibility of Fully Homomorphic Encryption in Clinical Diagnostics: Key Distribution and Computation Overhead. Journal of Medical Systems, 49(2), 102.

6. Islam, S., & Khan, R. (2022). Lightweight Cryptography for Secure E-Health Systems Using ECC. Computers & Security, 120, 102791.
7. Sharma, S., & Kaur, J. (2023). Biometric-Driven Encryption for Healthcare Data to Counter Replay and Spoofing Attacks. Health Informatics Journal, 29(1), 1–14.
8. Nehra, A., & Singh, R. (2024). Post-Quantum Cryptography Techniques for Next-Generation Healthcare Infrastructure. Future Internet, 16(1), 28.
9. Kumar, N., et al. (2022). Context-Aware Cryptographic Framework for Cloud-Based Healthcare Services. IEEE Transactions on Industrial Informatics, 18(3), 2045–2053.
10. Farooq, M., & Bhatia, A. (2023). Federated Key Distribution for Mobile Healthcare Networks. Journal of Information Security and Applications, 74, 103458.
11. Roy, A., et al. (2025). Adaptive Key Management and Anomaly Detection in Cyber-Resilient Healthcare Systems. ACM Transactions on Privacy and Security, 28(1), 1–22.
12. Zhang, Y., & Wang, L. (2020). Hybrid RSA-AES-Based Cryptosystem for Cloud-Hosted Medical Records. Procedia Computer Science, 171, 900–90.
13. Priyanka Kulkarni, & Dr. Swaroopa Shastri. (2024). Rice Leaf Diseases Detection Using Machine Learning. Journal of Scientific Research and Technology, 2(1), 17–22. https://doi.org/10.61808/jsrt81
14. Shilpa Patil. (2023). Security for Electronic Health Record Based on Attribute using Block-Chain Technology. Journal of Scientific Research and Technology, 1(6), 145–155. https://doi.org/10.5281/zenodo.8330325
15. Mohammed Maaz, Md Akif Ahmed, Md Maqsood, & Dr Shridevi Soma. (2023). Development Of Service Deployment Models In Private Cloud. Journal of Scientific Research and Technology, 1(9), 1–12. https://doi.org/10.61808/jsrt74
16. Antariksh Sharma, Prof. Vibhakar Mansotra, & Kuljeet Singh. (2023). Detection of Mirai Botnet Attacks on IoT devices Using Deep Learning. Journal of Scientific Research and Technology, 1(6), 174–187.
17. Dr. Megha Rani Raigonda, & Shweta. (2024). Signature Verification System Using SSIM In Image Processing. Journal of Scientific Research and Technology, 2(1), 5–11. https://doi.org/10.61808/jsrt79
18. Shri Udayshankar B, Veeraj R Singh, Sampras P, & Aryan Dhage. (2023). Fake Job Post Prediction Using Data Mining. Journal of Scientific Research and Technology, 1(2), 39–47.
19. Gaurav Prajapati, Avinash, Lav Kumar, & Smt. Rekha S Patil. (2023). Road Accident Prediction Using Machine Learning. Journal of Scientific Research and Technology, 1(2), 48–59.
20. Dr. Rekha Patil, Vidya Kumar Katrabad, Mahantappa, & Sunil Kumar. (2023). Image Classification Using CNN Model Based on Deep Learning. Journal of Scientific Research and Technology, 1(2), 60–71.
21. Ambresh Bhadrashetty, & Surekha Patil. (2024). Movie Success and Rating Prediction Using Data Mining. Journal of Scientific Research and Technology, 2(1), 1–4. https://doi.org/10.61808/jsrt78
22. Dr. Megha Rani Raigonda, & Shweta. (2024). Signature Verification System Using SSIM In Image Processing. Journal of Scientific Research and Technology, 2(1), 5–11. https://doi.org/10.61808/jsrt79
23. Dr. Megha Rani Raigonda, & Shweta. (2024). Signature Verification System Using SSIM In Image Processing. *Journal of Scientific Research and Technology*, *2*(1), 5–11. https://doi.org/10.61808/jsrt79
24. Jyoti, & Swaroopa Shastri. (2024). Gesture Identification Model In Traditional Indian Performing Arts By Employing Image Processing Techniques. *Journal of Scientific Research and Technology*, *2*(3), 29–33. https://doi.org/10.61808/jsrt89
25. M Manoj Das, & Dr. Swaroopa Shastri. (2025). Machine Learning Approaches for Early Brain Stroke Detection Using CNN . Journal of Scientific Research and Technology, 3(6), 243–250. https://doi.org/10.61808/jsrt248
26. Abhishek Ashtikar, & Dr. Swaroopa Shastri. (2025). A CNN Model For Skin Cancer Detection And Classification By Using Image Processing Techniques. *Journal of Scientific Research and Technology*, *3*(6), 251–263. https://doi.org/10.61808/jsrt250
27. Dr. Megha Rani Raigonda, & Anjali. (2025). Identification And Classification of Rice Leaf Disease Using Hybrid Deep Learning. *Journal of Scientific Research and Technology*, *3*(6), 93–101. https://doi.org/10.61808/jsrt231
28. Bhagyashree, & Dr. Swaroopa Shastri. (2025). A Machine Learning Approach To Classify Medicinal Plant Leaf By Using Random Forest And KNN. Journal of Scientific Research and Technology, 3(7), 100–115. https://doi.org/10.61808/jsrt261