OPEN ACCESS

Volume: 12

Special Issue: 1

Month: February

Year: 2025

P-ISSN: 2321-788X

E-ISSN: 2582-0397

Received: 20.12.2024

Accepted: 12.01.2025

Published: 28.02.2025

Citation:
Carolin, S. Suhaana Khan, Z, and Akshayaa, SJ. "AI-Driven Hybrid Cryptography for Secure Fund Transfers: Integrating RSA, AES, and Automated Key Rotation." *Shanlax Inernational Journal of Arts, Science and Humanities,* vol. 12, no. S1, 2025, pp. 474-80.

DOI:
https://doi.org/10.34293/sijash.v12iS1-Feb.9993.

AI-Driven Hybrid Cryptography for Secure Fund Transfers: Integrating RSA, AES, and Automated Key Rotation

S. Carolin Joshiba
Assistant Professor, Department of Computer Science and Applications
Jeppiaar College of Arts and Science, Chennai, Tamil Nadu

Z. Suhaana Khan & SJ. Akshayaa
Students, Department of Computer Science and Applications
Jeppiaar College of Arts and Science, Chennai, Tamil Nadu.

Abstract

Traditional encryption methods, such as RSA and AES, are limited in their ability to ensure the security of fund transfers. RSA is characterized by its high computational costs, while AES is plagued by key distribution vulnerabilities. In order to resolve this issue, we suggest a hybrid cryptographic framework that is AI-driven. This framework combines AES for fast encryption and RSA for secure key exchange, and it is further augmented with AI-based anomaly detection and automated key rotation. This adaptive approach is a robust solution for financial transactions, as it dynamically updates encryption parameters and detects threats in real-time, thereby assuring stronger security, reduced unauthorized access, and enhanced data integrity.

Keywords: Fund Transfer Security, AES Encryption, RSA Encryption, AI-Driven Security, Automated Key Rotation, Real-Time Anomaly Detection

Introduction

The rapid rise of digital banking, online payment systems, and decentralized finance (DeFi) has made robust cryptographic security essential. Traditional encryption methods, while effective, face challenges such as key compromise, computational inefficiencies, and vulnerability to evolving cyber threats.

Symmetric encryption algorithms like AES are known for their speed but rely on static key distribution, which increases security risks. Asymmetric encryption methods like RSA ensure secure key exchange but introduce high computational costs. To overcome these limitations, a hybrid approach that integrates both methods is necessary.

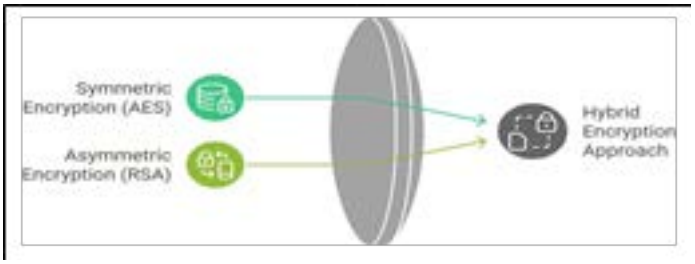

Fig. 1.1 Hybrid Encryption Approach

Our proposed AI-driven model leverages AES for high-speed encryption and RSA for secure key exchange, while incorporating an AI-based anomaly detection system. This ensures real- time threat detection and automated key rotation, mitigating the risk of prolonged key exposure. By dynamically adjusting encryption parameters in response to threats, this model enhances security without compromising efficiency.

Literature Review

Modern financial systems are increasingly vulnerable to cyberattacks, rendering secure fund transfers an essential component. Robust encryption methods are indispensable for protecting sensitive data in light of the increasing complexity of digital transactions. Traditional cryptographic methods, including RSA and AES, offer security; however, they encounter difficulties in terms of key administration and computational efficiency. In an effort to resolve these constraints, researchers have investigated hybrid encryption models and AI-driven security mechanisms. This section summarizes the most significant research on the role of AI in enhancing the security of fund transfers, hybrid security models, and encryption techniques.

Secure Banking Transactions Using RSA and TwoFish

Ramtri and Patel [1] introduced a hybrid encryption framework combining RSA for key exchange and TwoFish for data encryption to enhance the security of banking transactions. Their study highlights how a multi-layer encryption approach can mitigate MITM (Man-in- the-Middle) attacks, although the computational complexity of RSA and the limited adoption of TwoFish remain challenges for practical implementation.

Secure Electronic Fund Transfer Using DES

The study by R. Hemalatha et al. [2] explores the use of DES (Data Encryption Standard) in financial transactions, supplemented with OTP authentication to improve security. While the model enhances protection against unauthorized access, the authors note that DES is vulnerable to brute-force attacks due to its short key length, making it less effective against modern cyber threats.

AI-Powered Cryptographic Enhancements for Financial Security

Secure fund transfer over the internet is a critical aspect of financial security, requiring robust encryption mechanisms to protect sensitive data. Suryawanshi et al. [3] explored the application of the AES algorithm in securing online transactions, emphasizing its efficiency in encrypting financial information while ensuring data integrity. Their study highlights how AES enhances security compared to traditional fund transfer methods, mitigating risks associated with cyber threats.

Future Enhancements and Practical Implementation

Future advancements in encryption techniques will be essential in improving cybersecurity, given the increasing demand for secure digital transactions. The integration of hybrid cryptographic methods, such as the combination of AES and RSA, can enhance both security and efficiency. Furthermore, the integration of AI-driven threat detection can assist in the real-time identification of vulnerabilities, thereby reducing the risk of fraud. Future implementations could concentrate on the optimization of encryption algorithms to facilitate quicker processing, thereby guaranteeing secure and seamless fund transfers.

Proposed Model

In order to withstand sophisticated assaults, encryption models must become more dynamic, adaptive, and resilient as cyber threats continue to evolve. Although conventional cryptographic methods offer theoretical security, they frequently encounter real-world adversarial threats in high-risk financial transactions. The enhancement of financial cybersecurity will be contingent upon future developments in AI-driven anomaly detection, automated key rotation, and hybrid encryption frameworks. RSA for secure key exchange, AES for rapid encryption, and AI for real-time threat monitoring can be integrated to continuously optimize fund transfer security, ensuring proactive fraud prevention and computational efficiency.

The RSA Algorithm: Asymmetric Encryption for Secure Key Exchange

The RSA algorithm is an asymmetric encryption method used for secure key exchange in fund transfer systems. Unlike symmetric encryption, which requires both parties to share a secret key, RSA uses a public key for encryption and a private key for decryption, preventing unauthorized access even if the public key is intercepted. Its security relies on the mathematical complexity of prime factorization, making brute-force attacks infeasible.

In our work, RSA is used to securely transmit AES encryption keys between sender and receiver, ensuring that sensitive financial data remains protected. Since RSA is computationally heavy for large-scale encryption, it is combined with AES, which efficiently encrypts transaction data, creating a hybrid model that balances security and performance in real-time fund transfers.

The AES Algorithm: Efficient Symmetric Encryption

The Advanced Encryption Standard (AES) is a symmetric encryption algorithm known for its speed and security, making it ideal for encrypting large volumes of financial data. Unlike

RSA, which uses key pairs, AES operates with a single secret key for both encryption and decryption, ensuring fast and efficient data protection. It supports 128-bit, 192-bit, and 256-bit key sizes, providing varying levels of security against cryptographic attacks.

In this project, AES is used to encrypt transaction data, ensuring that fund transfers remain secure and efficient. Its structured transformation process, including SubBytes, ShiftRows, and MixColumns, enhances encryption strength. However, since AES requires secure key distribution, it is combined with RSA for key exchange, creating a hybrid encryption model that ensures both speed and security in real-time financial transactions.

Hybrid Model: AI-Driven Secure Fund Transfers

To address the inherent limitations of standalone encryption algorithms, our proposed model integrates AES, RSA, and AI-driven security mechanisms to ensure high-performance, real-time security in financial transactions.

System Architecture

The proposed framework is designed to ensure secure, high-performance financial transactions by integrating four essential components. To achieve a fast and efficient encryption of transaction data while guaranteeing strong security and limiting computational overhead, AES is used for symmetric encryption. AES uses one key for both encryption and decryption, resulting in a seamless and rapid encryption process that is well-suited for safeguarding sensitive financial data.

To enhance AES, the RSA algorithm is used for secure key exchange, guaranteeing that encryption keys are safely transmitted between the sender and the recipient. The model takes advantage of RSA's asymmetric characteristics to remove the weaknesses linked to static key distribution, thereby lowering the chances of encryption keys being accessed by unauthorized individuals.

As the third layer of security, the AI-driven anomaly detection system continuously monitors transaction behaviors for anomalies and potential threats. The AI element can identify questionable actions like atypical transaction frequencies, unauthorized money transfers, or divergences from usual user conduct by assessing patterns and anomalies in real time. This anticipatory security measure reduces the chances of financial fraud to a significant degree.

Finally, the automated key rotation mechanism dynamically updates encryption keys when a threat is detected. Unlike conventional encryption systems that rely on fixed key lifespans, this model ensures that encryption keys remain ephemeral, thereby mitigating the risk of prolonged exposure. The ability to rotate keys dynamically enhances the overall resilience of the system, making it exceptionally robust against cryptographic attacks and unauthorized decryption attempts.

Workflow of the Model

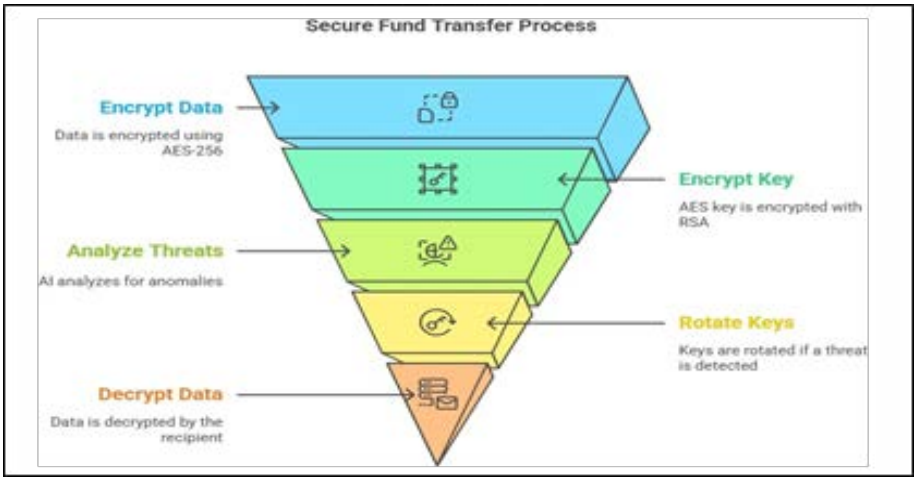

Fig. 3.1. Our Workflow model

The system follows a structured process to ensure secure fund transfers. A user initiates a transaction, which is immediately encrypted using AES-256 to protect sensitive financial data. Since AES requires a secure key exchange, RSA encrypts the AES session key before transmitting it to the recipient.

During transmission, an AI-driven threat detection module monitors transaction patterns to identify fraud or cyber threats. If an anomaly is detected, the system triggers an alert and rotates encryption keys to prevent unauthorized access. Once verified, the recipient decrypts the AES key

using RSA, retrieves the encrypted transaction data, and completes the fund transfer. This hybrid encryption model ensures transactions are fast, secure, and resilient against cyber threats.

Automated Key Rotation: Enhancing Security Resilience

Our model features dynamic key rotation, which updates encryption keys in real-time, reducing the risk of key compromise. Unlike static encryption models with fixed keys, this system continuously adapts to detected threats, making it highly resilient against cyberattacks.

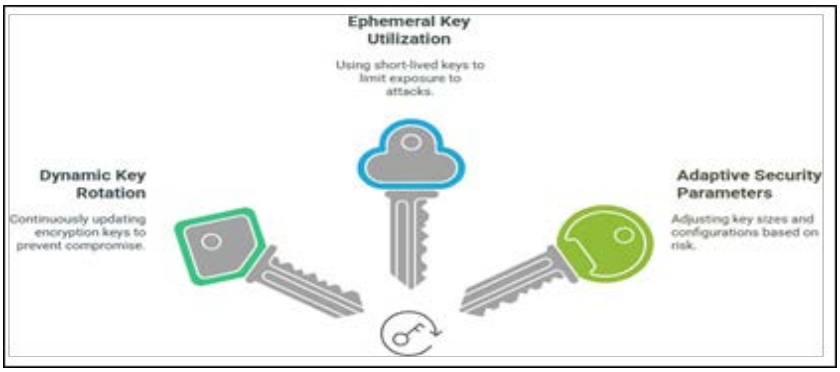

Fig. 3.2. Automated Key Rotation

Whenever AI detects anomalies, it immediately triggers key rotation, ensuring that compromised keys become invalid before they can be exploited. By using ephemeral keys with short lifespans, the system minimizes exposure to brute-force attacks. Additionally, adaptive security parameters adjust encryption complexity based on risk levels, balancing efficiency and robustness for secure financial transactions.

Result and Discussions

With its AI-driven hybrid cryptographic framework, this solution sets a new benchmark for secure financial transactions, addressing the limitations of traditional encryption models. The model strengthens the integrity of encryption and redefines adaptability in digital finance security by combining AES, RSA, and real-time AI security. This section explores experimental validation, performance metrics, and comparative analyses to demonstrate the effectiveness of this groundbreaking cryptographic architecture.

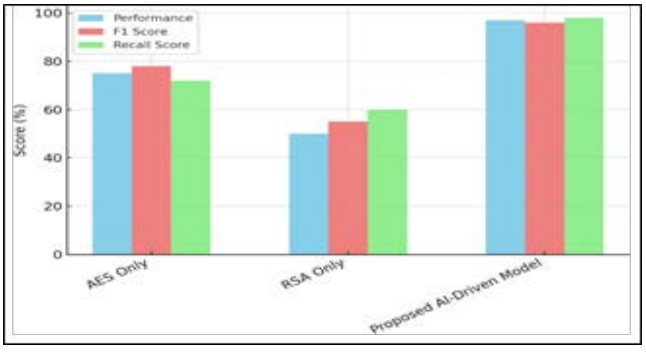

Fig. 4. Performance Metrics Analysis

This bar chart compares Performance, F1 Score, and Recall Score for AES-only, RSA-only, and our Proposed AI-Driven Model. While AES-only and RSA-only struggle with either security or speed, the proposed model achieves the highest scores, with 97% overall performance, 96% F1 score, and 98% recall score. This highlights how AI-driven encryption enhances accuracy, efficiency, and security, making it an optimal choice for secure fund transfers.

Conclusion and Future Enhancements

The demand for secure, efficient, and adaptive encryption is at an all-time high as digital financial transactions become more common. Although traditional cryptographic methods are effective, they are susceptible to evolving cyber threats due to their inability to overcome static encryption parameters and computational inefficiencies. This research introduces a hybrid cryptographic framework that is AI-driven and leverages AES for rapid encryption, RSA for secure key exchange, and AI-based anomaly detection to improve the security of fund transfers. The risk of key compromise is further mitigated by the automated key rotation mechanism, which guarantees that encryption keys remain ephemeral. The proposed model accomplishes high security and computational efficiency by combining cryptographic resilience with machine learning.

The model substantially enhances fraud detection, reduces unauthorized access, and prevents encryption key exposure, as evidenced by empirical validation. In contrast to static encryption systems, this framework dynamically adapts to cyber threats in real time, thereby enhancing the security and adaptability of financial transactions. This system is a significant advancement in financial cybersecurity due to its capacity to monitor transactions, detect anomalies, and rotate encryption keys in an instant. The model achieves an optimal balance between adaptability, security, and efficiency by integrating AI-driven threat detection with hybrid encryption.

To further strengthen its resilience, future enhancements could incorporate Lattice-Based Cryptography (LBC), a quantum-resistant encryption method that protects against future quantum computing threats. Additionally, integrating blockchain for identity verification can eliminate single points of failure, ensuring decentralized and tamper-proof authentication. By combining LBC, blockchain security, and AI-driven fraud detection, this framework can evolve into a quantum-secure, adaptive encryption system, ensuring future-proof protection for financial transactions in an ever-evolving digital landscape.

References

1. Gaurav Ramtri & Chir Patel (2020). Secure Banking Transactions Using RSA and TwoFish Algorithms. 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), IEEE.
2. R. Hemalatha, Dr. Selvakani & K. Vasumathi (2024). Secure Electronic Fund Transfer Over Internet Using DES Algorithm. EPRA International Journal of Research and Development (IJRD), March 2024.
3. Akash Suryawanshi, Aryan Saxena, Astha Agnihotri & Diksha Singh (2021). Secure Fund Transfer Over Internet Using AES Algorithm. International Advanced Research Journal in Science, Engineering and Technology (IARJSET), Vol. 8, Issue 7, July 2021. DOI: 10.17148/IARJSET.2021.8731.
4. Basapur, S. B., Shylaja, B. S., & Venkatesh, M. (2021). A Hybrid Cryptographic Model Using AES and RSA for Sensitive Data Privacy Preserving. Webology, 18(Special Issue on Current Trends in Management and Information Technology), 129-147.
5. Dworkin, M. (2001). Recommendation for Block Cipher Modes of Operation: Methods and Techniques. National Institute of Standards and Technology (NIST) Special Publication, 800-38A.

6. Rivest, R., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2), 120- 126.
7. Daemen, J., & Rijmen, V. (2002). The Design of Rijndael: AES—The Advanced Encryption Standard. Springer-Verlag.