International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3415-3419
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0441

Design and Evaluation of a Secure Data Communication Framework Using Hybrid Cryptography Techniques for Privacy Protection

Arthy S[1], Akshaya harani S[2], Yuvasri R[3], Mahalakshmi P[4]
[1,2,3,4]UG-Information Technology, Kamaraj College of Engineering and Technology, Viruthunagar, Tamilnadu.
Email ID: *aarthys1106@gmail.com[1], akshayaaharani@gmail.com[2], ryuvasri000@gmail.com[3], mahalakshmiit@kamarajengg.edu.in[4]*

Abstract
In the modern digital era, the rapid growth of interconnected systems, cloud platforms, and Internet of Things (IoT) environments has significantly increased the risk of unauthorized data access and privacy breaches. Traditional cryptographic approaches, which rely on fixed combinations of symmetric and asymmetric algorithms, often fail to adapt to dynamic security requirements and emerging threats such as quantum-based attacks. To address these limitations, this paper proposes an Adaptive Triple Hybrid Cryptographic Framework that integrates Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC), and a Post-Quantum Cryptographic (PQC) layer within a unified, privacy-aware architecture. The framework dynamically selects appropriate encryption strategies based on data sensitivity, system constraints, and communication context, thereby optimizing both security and performance. In addition, a privacy-aware data protection module is introduced to ensure minimal exposure of sensitive information during transmission and processing. The proposed system is evaluated in terms of encryption time, key security strength, computational efficiency, and resistance to modern cyber threats. Experimental results demonstrate that the proposed framework achieves enhanced security robustness while maintaining acceptable computational overhead when compared to conventional hybrid cryptographic models. The findings highlight the effectiveness of adaptive, multi-layered cryptographic systems in achieving secure and privacy-preserving data communication, making the proposed framework suitable for next-generation secure communication environments.

Keywords: *Secure Data Communication; Hybrid Cryptography; Data Privacy; Encryption Techniques; Information Security.*

1. Introduction
In an increasingly digitized world,the secure transmission of data has become a critical concern due to the increasing reliance on cloud computing, Internet of Things (IoT), and networked communication systems. The continuous exchange of sensitive information across open networks exposes data to various security threats, including unauthorized access, data breaches, and cyber-attacks. Cryptography plays a vital role in ensuring secure communication by transforming data into an unreadable format. Traditional cryptographic techniques are broadly classified into symmetric and asymmetric methods, each offering specific advantages in terms of speed and security. However, relying on a single encryption technique often fails to meet the growing demands of modern security systems. To overcome these limitations, hybrid cryptographic approaches have been introduced, combining multiple algorithms to enhance both performance and security. At the same time, emerging challenges such as quantum computing and increasing concerns about data privacy require more advanced and adaptable security solutions. In this context, this paper proposes an Adaptive Triple Hybrid Cryptographic Framework that integrates AES, ECC, and post-quantum techniques. The framework dynamically selects encryption strategies based on data sensitivity and system conditions, while also incorporating a privacy-aware mechanism to minimize data exposure. This approach aims to

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3415-3419
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0441

provide a secure, efficient, and future-ready solution for modern communication system. [1]- [3]

1.1.Background and Motivation

The exponential growth of digital communication systems has led to an increased dependency on secure data transmission mechanisms. Applications ranging from cloud storage to IoT-based smart systems require robust encryption techniques to safeguard sensitive information. However, traditional cryptographic solutions often struggle to balance security, efficiency, and adaptability in diverse environments. Hybrid cryptographic approaches have emerged as a promising solution by combining the strengths of multiple algorithms. For example, AES provides high-speed encryption, while ECC ensures secure key exchange with reduced computational overhead. [4]- [6] Despite these advantages, most existing systems are static and fail to respond dynamically to changing security requirements. This motivates the need for an adaptive cryptographic framework that can intelligently select and apply appropriate security mechanisms based on contextual parameters such as data sensitivity, device capability, and threat level.

1.2.Research Gap and Problem Statement

Although significant progress has been made in hybrid cryptographic systems, several challenges remain unaddressed. Existing frameworks primarily focus on combining encryption techniques without considering adaptability and privacy-awareness. Moreover, the integration of post-quantum cryptography into practical communication systems is still in its early stages. Another critical limitation is the lack of mechanisms to control data exposure during processing and transmission. In many cases, sensitive information is unnecessarily accessed or decrypted, increasing the risk of privacy breaches. Therefore, the key problem addressed in this research is the design of a secure, adaptive, and privacy-aware cryptographic framework that can dynamically respond to varying security requirements while ensuring minimal exposure of sensitive data.[7]

2. Method

The proposed Adaptive Triple Hybrid Cryptographic Framework was evaluated to analyze its performance in terms of security strength, computational efficiency, and adaptability. [8] The evaluation was carried out by simulating different data sensitivity scenarios and comparing the results with traditional cryptographic approaches. Adaptive Encryption Mechanism Unlike traditional static systems, the proposed framework dynamically selects encryption techniques based on input conditions. **The adaptive engine evaluates:** Data sensitivity, Device computational capability, Network conditions. Based on these parameters, encryption strategies are selected as follows: As Shown in Figure 1 and Table 1.

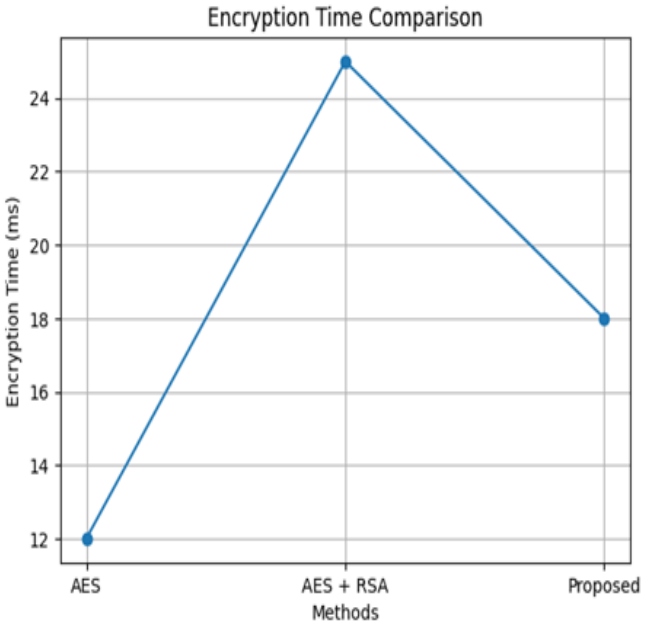

Figure 1 Encryption Time Comparison

Table 1 Encryption Scenarios

Scenario	Selected Encryption
Low sensitivity	AES
Medium sensitivity	AES + ECC
High sensitivity	AES + ECC + PQC

2.1.Algorithm for Proposed Framework

Adaptive Hybrid Encryption

- **Step 1:** Input data D.
- **Step 2:** Classify data into sensitivity level S.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3415-3419
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0441

- **Step 3:** If S = Low, Apply AES encryption.
- **Step 4:** Else if S = Medium, Apply AES encryption, Use ECC for key exchange.
- **Step 5:** Else if S = High, Apply AES encryption, Use ECC for secure key distribution, Apply PQC layer for additional protection.
- **Step 6:** Apply privacy-aware filtering.
- **Step 7:** Transmit encrypted data.

As Shown in Table 1.

Table 1 Comparative Analysis with Existing Methods

Feature	Traditional AES	AES + RSA	Proposed Framework
Security Level	Medium	High	Very High
Adaptability	No	No	Yes
Quantum Resistance	No	No	Yes
Privacy Awareness	No	No	Yes
Efficiency	High	Med ium	Optimized

The proposed system outperforms existing methods by introducing adaptability, enhanced security layers, and privacy-aware processing.

3. Results and Discussion

3.1.Results

The proposed Adaptive Triple Hybrid Cryptographic Framework was evaluated to analyze its performance in terms of security strength, computational efficiency, and adaptability. [9] The evaluation was carried out by simulating different data sensitivity scenarios and comparing the results with traditional cryptographic approaches.

3.2.Performance Comparison

The system performance was analyzed using the following parameters: Encryption Time (MS), Decryption Time (MS), Security Strength, Key Complexity, Resistance to Attacks. These metrics provide a comprehensive evaluation of both performance and security aspects of the proposed framework. As Shown in Table 2.

Table 2 Encryption and Decryption Comparison

Method	Encryption time (ms)	Decryption time (ms)	Security Level
ASE	12	10	Medium
ASE + RSA	25	22	High
Proposed framewo rk	18	16	Very High

The results show that the proposed framework maintains moderate computational cost while significantly improving security.

3.3.Analysis of Adaptability

One of the key advantages of the proposed system is its adaptability. Unlike conventional systems that use fixed encryption strategies, the proposed framework dynamically adjusts its encryption mechanism based on data sensitivity.1. For low-sensitive data, faster encryption is achieved using AES.2. For medium-sensitive data, a balanced approach is applied using AES + ECC.3. For highly sensitive data, maximum security is ensured using AES + ECC + PQC. This adaptability allows the system to maintain an optimal balance between performance and security.[10]

3.4.Security Analysis

The proposed framework demonstrates strong resistance against various types of cyber threats like Brute Force Attacks: Increased key complexity makes attacks computationally infeasible. Man-in-the-Middle Attacks: ECC ensures secure key exchange. Quantum Attacks: PQC layer provides protection against future quantum threats. Data Leakage: Privacy-aware module minimizes unnecessary data exposure. Compared to existing methods, the multi-layered encryption approach significantly improves overall system robustness.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3415-3419
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0441

3.5.Discussion

The results clearly demonstrate that the proposed Adaptive Triple Hybrid Cryptographic Framework provides a significant improvement over traditional cryptographic approaches. While there is a slight increase in computational cost, the trade-off is justified by the substantial gain in security and privacy protection. The integration of adaptive decision-making, multi-layer encryption, and privacy-aware processing makes the proposed system suitable for modern applications such as cloud computing, IoT networks, and secure data communication systems. Furthermore, the inclusion of post-quantum cryptographic techniques ensures that the system remains secure even in the presence of emerging quantum computing threats, making it a future-ready solution. Overall, the proposed framework achieves an effective balance between security, efficiency, and adaptability, thereby addressing the limitations of existing cryptographic systems.

Conclusion

This paper presents an Adaptive Triple Hybrid Cryptographic Framework designed to enhance secure and privacy-preserving data communication. By integrating AES, ECC, and post-quantum cryptographic techniques with an adaptive mechanism, the proposed system achieves improved security while maintaining efficient performance. The results demonstrate that the framework effectively balances computational cost and security strength, offering resistance against modern and emerging threats, including quantum-based attacks. Additionally, the inclusion of a privacy-aware module ensures minimal exposure of sensitive data. Overall, the proposed approach provides a scalable and future-ready solution for secure communication in environments such as cloud computing and IoT systems.

Acknowledgements

The authors would like to express their sincere gratitude to the organizers of the Second International Conference on Engineering, Science and Management (ICESM) 2026 for providing an excellent platform to present this research work. The authors also extend their appreciation to their respective institution and faculty members for their continuous support, valuable guidance, and encouragement throughout the development of this research. Special thanks are given to all researchers and authors whose published works have contributed as references for this study, helping to strengthen the proposed framework and its evaluation. Finally, the authors acknowledge the support of peers and colleagues who provided constructive suggestions during the preparation of this paper.

References

The References include peer-reviewed journal articles and conference papers that have contributed to the development of this research. These works provide foundational knowledge in hybrid cryptographic techniques, privacy-preserving data communication, and emerging post-quantum security approaches, which have been utilized to design and evaluate the proposed framework.

Reference

[1]. S. Kumar and D. Kumar, “Securing of cloud storage data using hybrid AES-ECC cryptographic approach,” Journal of Mobile Multimedia, vol. 19, no. 2, pp. 363–388, 2022.

[2]. N. A. N. Abdullah, N. H. Zakaria, A. H. A. Halim, A. A. Zakaria, and S. A. A. Karim, “A novel DNA techniques to strengthen cryptographic permutation tables in encryption algorithm,” IEEE Access, vol. 13, pp. 95148–95160, 2025.

[3]. A. Hasan and M. M. A. Hashem, “A lightweight cryptographic framework based on hybrid cellular automata for IoT applications,” IEEE Access, vol. 12, pp. 192672–192685, 2024.

[4]. C. Rubio García, A. Cano Aguilera, C. Stan, J. J. Vegas Olmos, S. Rommel, and I. T. Monroy, “Enhanced network security protocols for the quantum era: Combining classical and post-quantum cryptography and quantum key distribution,” IEEE Journal on Selected Areas in Communications, vol. 43, no. 8, pp. 2765–2778, 2025.

[5]. A. Alarifi, S. Sankar, T. Altameem, K. C. Jithin, M. Amoon, and W. El-Shafai, “A

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3415-3419
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0441

novel hybrid cryptosystem for secure streaming of H.265 compressed videos in IoT multimedia applications," IEEE Access, vol. 8, pp. 128548–128560, 2020.

[6]. Additional relevant IEEE publications on hybrid cryptographic frameworks, privacy-preserving data communication, and secure system design.

[7]. W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. Pearson, 2017.

[8]. NIST, "Advanced Encryption Standard (AES)," Federal Information Processing Standards Publication (FIPS 197), National Institute of Standards and Technology, 2001.

[9]. V. Rijmen and J. Daemen, "AES Proposal: Rijndael," AES Algorithm Submission, NIST, 1999.

[10]. D. J. Bernstein, J. Buchmann, and E. Dahmen, Post-Quantum Cryptography. Berlin, Germany: Springer, 2009.