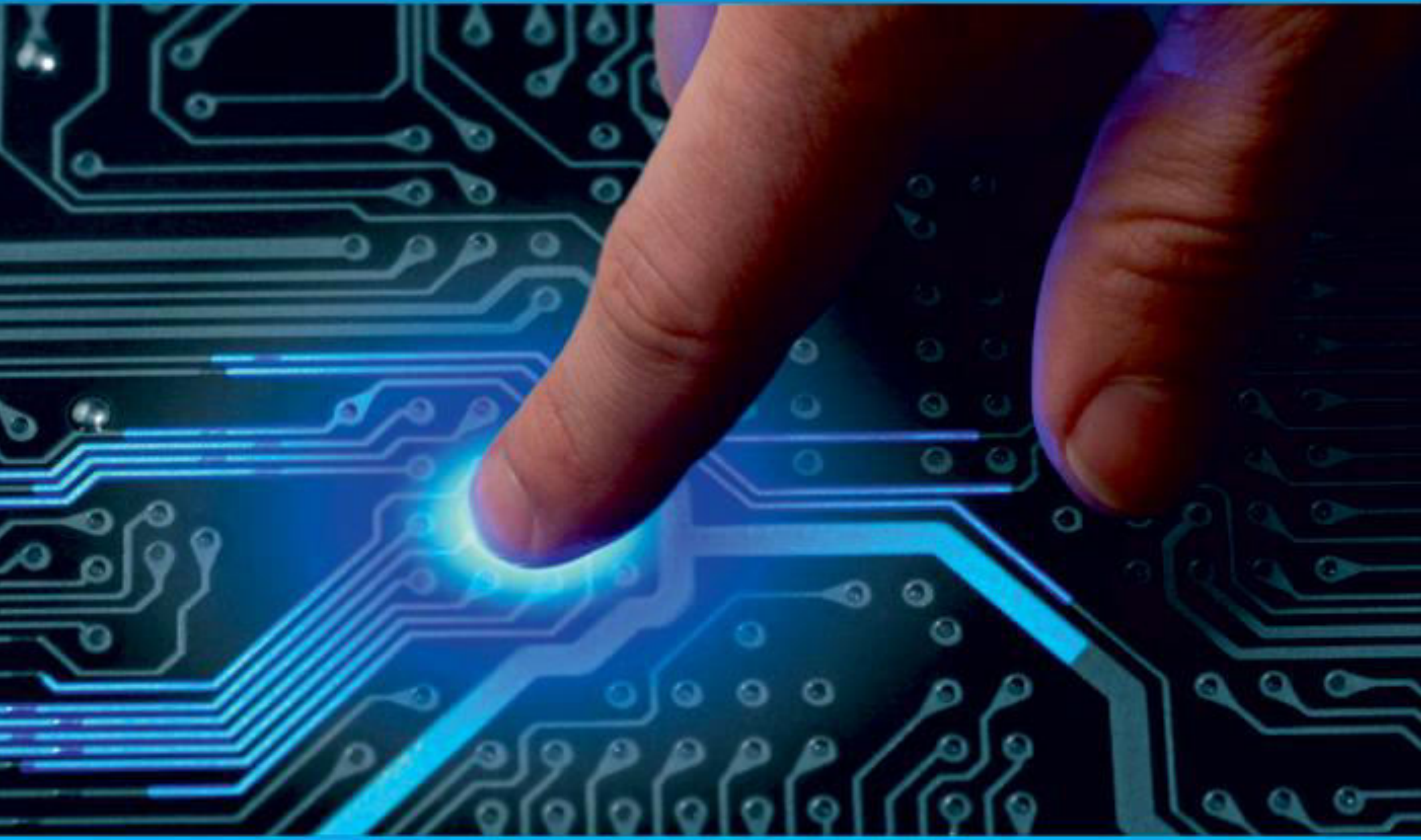
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Special Issue 1, March 2024

1st International Conference on Machine Learning, Optimization and Data Science

Organized by

Department of Computer Science and Engineering, Baderia Global Institute of Engineering and Management, Jabalpur, India

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 || Monthly Peer Reviewed & Refereed Journal |

| "1st International Conference on Machine Learning, Optimization and Data Science"|

Organized by

| Department of Computer Science and Engineering, Baderia Global Institute of Engineering and Management, Jabalpur|

|| Volume 12, Special Issue 1, March 2024 ||

Fusing Advanced Encryption Standard (AES) with Rivest-Shamir-Adleman (RSA) Encryption Algorithms in Extended Reality (XR) Systems Techniques

Rashi Chouksey[1], **Prof. Saurabh Sharma**[2]

Baderia Global Institute of Engineering & Management, Jabalpur, India

ABSTRACT: The integration of Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) encryption algorithms into Extended Reality (XR) systems provides a robust framework for securing data transmission and preserving user privacy in immersive environments. As XR technologies expand across various sectors like healthcare, education, and entertainment, ensuring the security of sensitive information, including personal data and real-time interactions, becomes critical. This paper proposes a hybrid encryption model that combines the speed and efficiency of AES with the robust security of RSA to protect communication and prevent unauthorized access in XR environments. By utilizing both symmetric and asymmetric encryption methods, this hybrid framework addresses the growing need for secure and scalable solutions in XR systems. The experimental results demonstrate that the proposed approach significantly enhances data security without compromising system performance, making it a promising solution for the future of secure XR applications.

KEYWORDS: Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), Hybrid Encryption, Extended Reality (XR), Data Security

I. INTRODUCTION

1.1 Overview of XR Systems and the Importance of Data Security: Extended Reality (XR) technologies, encompassing Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR), have revolutionized how users interact with digital environments, offering immersive experiences across sectors like healthcare, education, gaming, and industrial training. These systems rely on real-time data processing, transmission, and storage to deliver seamless and personalized user experiences. However, the increasing reliance on sensitive data, including personal information, biometric details, and location data, makes XR systems vulnerable to cybersecurity threats such as data breaches, unauthorized access, and malicious attacks. As XR adoption grows, ensuring robust data security becomes paramount to safeguard users and maintain trust in these technologies.

1.2 Need for Secure Communication in XR Environments: In XR systems, communication between devices, servers, and users involves transmitting critical data over networks, often in real time. This includes interactions with virtual objects, user authentication details, and sensitive data exchanges for collaborative environments. Without proper encryption, these data transmissions are susceptible to interception, eavesdropping, and tampering. Existing security solutions often fail to provide the necessary balance between high-level security and real-time performance, which is essential for XR applications. Therefore, a more secure, efficient, and scalable encryption approach is needed to protect communication in XR environments.

1.3 Purpose and Scope of the Study: This study aims to address the growing security concerns in XR systems by proposing a hybrid encryption framework that fuses Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) algorithms. By leveraging the speed and efficiency of AES for bulk data encryption and the robust security of RSA for key management, the proposed model seeks to enhance the overall security of XR systems while maintaining real-time performance. This research explores the implementation of this hybrid encryption technique, evaluates its effectiveness in securing XR environments, and compares its performance with traditional encryption methods. The findings are expected to contribute to the development of secure and scalable XR systems for various applications.

II. BACKGROUND AND LITERATURE REVIEW

2.1 Overview of AES and RSA Encryption Algorithms: The Advanced Encryption Standard (AES) is a widely used symmetric encryption algorithm known for its speed and efficiency in securing large volumes of data. It employs fixed block sizes (128 bits) and supports key lengths of 128, 192, or 256 bits, ensuring robust protection against brute-force attacks. On the other hand, Rivest-Shamir-Adleman (RSA) is a public-key encryption algorithm that uses asymmetric cryptography to provide secure key exchanges and data encryption. RSA's strength lies in its reliance on the mathematical complexity of prime factorization, making it a robust choice for secure communication. While AES excels in performance for bulk data encryption, RSA provides high security for key management and digital signatures.

2.2 Applications of AES and RSA in Data Security: AES and RSA encryption algorithms have been extensively adopted across diverse domains. AES is frequently used for securing sensitive information in banking, healthcare, and cloud storage, where fast encryption and decryption are critical. RSA, on the other hand, is prominent in secure email communication, digital certificates, and virtual private networks (VPNs) due to its ability to securely exchange cryptographic keys over unsecured channels. Combining AES and RSA is a well-established practice for hybrid encryption systems, ensuring secure and efficient communication in applications such as e-commerce, blockchain, and secure file sharing.

2.3 Previous Research on Encryption in XR Systems: The increasing adoption of XR systems has sparked interest in developing encryption frameworks tailored to their unique requirements. Previous research highlights the need for balancing robust security with low-latency performance to ensure seamless user experiences in XR environments. Some studies propose using AES for real-time data encryption due to its speed, while others advocate RSA for its superior security in key exchanges. However, challenges such as computational overhead, scalability, and compatibility with XR devices remain prevalent. The fusion of AES and RSA has been explored in other domains but requires further investigation to address XR-specific security concerns. This study builds on prior research by implementing and evaluating a hybrid encryption model that combines AES and RSA to secure XR systems effectively.

III. PROBLEM STATEMENT

3.1 Security Challenges in XR Environments: Extended Reality (XR) systems involve the integration of virtual, augmented, and mixed reality technologies to create immersive digital experiences. These systems process large volumes of sensitive data, including personal information, real-time user interactions, and environmental data, making them highly vulnerable to security breaches. Key challenges include the risk of unauthorized data access, interception of communications, and malicious attacks that can compromise the privacy and integrity of user information. Additionally, the real-time nature of XR applications necessitates encryption methods that balance robust security with minimal latency, ensuring seamless performance without compromising the user experience.

3.2 Limitations of Existing Security Solutions: Current security solutions for XR systems often rely on traditional encryption methods, which may not fully address the unique demands of immersive environments. Symmetric encryption algorithms like AES offer speed but may struggle with secure key distribution, while asymmetric methods like RSA ensure secure key exchange but are computationally intensive for large-scale data encryption. Existing hybrid encryption models often lack optimization for XR-specific scenarios, resulting in either reduced security or increased latency. These limitations underscore the need for a tailored hybrid encryption framework that can provide robust security, efficient performance, and scalability in XR environments.

IV. PROPOSED HYBRID ENCRYPTION MODEL

4.1 Concept of Hybrid Encryption: Hybrid encryption is a combination of symmetric and asymmetric encryption techniques, designed to leverage the advantages of both approaches. Symmetric encryption methods, such as AES, provide high-speed encryption and are suitable for processing large volumes of data. On the other hand, asymmetric encryption methods, such as RSA, ensure secure key exchange over untrusted networks. By integrating these methods, hybrid encryption offers a robust framework that addresses the limitations of each technique when used in isolation, ensuring both performance and security in data protection.

4.2 Integration of AES and RSA in XR Systems: The integration of AES and RSA encryption algorithms in XR systems addresses critical security and performance needs for immersive applications. In this approach, RSA is used to securely exchange the session key, ensuring that it cannot be intercepted during transmission. AES then utilizes this session key to encrypt the bulk of the data, such as real-time user interactions, multimedia files, and virtual environment configurations. This dual-layered encryption not only protects against unauthorized access but also ensures low-latency performance, which is essential for seamless XR experiences. The result is a secure and efficient framework tailored to the high-demand requirements of XR systems.

4.3 Design and Architecture of the Hybrid Model

- **Key Generation Module:** The key generation module forms the backbone of the hybrid encryption model by creating secure cryptographic keys. RSA generates a pair of public and private keys for asymmetric encryption, which are used for securely exchanging session keys. Simultaneously, AES generates a symmetric session key that will be used for encrypting the actual XR data. This dual-key system ensures both the security of the key exchange process and the efficiency of data encryption and decryption.

- **Encryption Process:** During the encryption phase, the AES session key is first encrypted using RSA’s public key. This step ensures that the session key can be transmitted securely without the risk of interception. Once the session key is exchanged, the actual data, such as XR inputs and multimedia streams, is encrypted using AES. The combination of secure key exchange and rapid data encryption ensures a robust protection mechanism for all transmitted information in XR environments.

- **Decryption Process:** The decryption process reverses the encryption steps, ensuring secure and efficient data access. The recipient first decrypts the AES session key using RSA's private key, guaranteeing that only authorized users can access the key. After obtaining the session key, the recipient uses AES to decrypt the transmitted data, restoring the original content. This two-step process ensures data integrity and security, even when transmitted over potentially insecure networks.

- **System Architecture:** The architecture of the proposed hybrid encryption model includes three primary layers:
  - **Input Layer:** This layer collects real-time data, including user interactions, multimedia content, and virtual environment parameters, ensuring all inputs are securely processed.
  - **Processing Layer:** At this stage, the hybrid encryption model applies AES for data encryption and RSA for key management, ensuring secure transmission and storage of XR data.
  - **Output Layer:** The final layer decrypts and delivers the original data to the recipient's XR application, ensuring a seamless and secure user experience.

V. METHODOLOGY

5.1 Flowchart for Algorithm

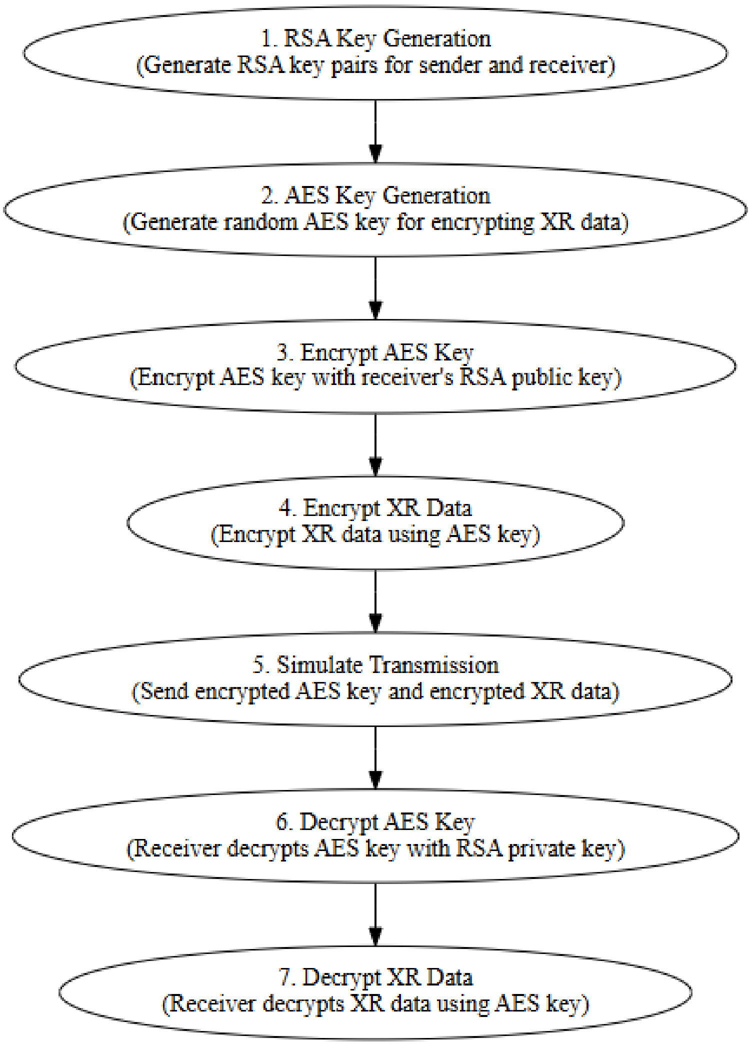

1. RSA Key Generation
(Generate RSA key pairs for sender and receiver)
2. AES Key Generation
(Generate random AES key for encrypting XR data)
3. Encrypt AES Key
(Encrypt AES key with receiver's RSA public key)
4. Encrypt XR Data
(Encrypt XR data using AES key)
5. Simulate Transmission
(Send encrypted AES key and encrypted XR data)
6. Decrypt AES Key
(Receiver decrypts AES key with RSA private key)
7. Decrypt XR Data
(Receiver decrypts XR data using AES key)

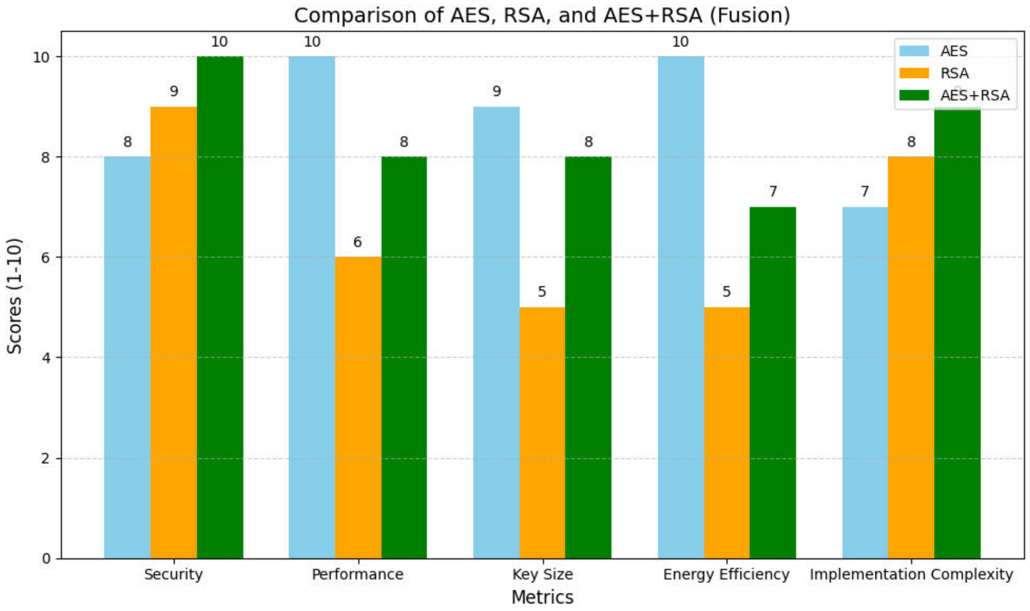
FIGURE 1 ALGORITHM FLOW CHART FOR SECURING XR ENVIRONMENTS AGAINST VARIOUS CYBER THREATS

5.2 Data Table: Comparison of AES, RSA, and AES+RSA (Fusion)

Metric	AES	RSA	AES+RSA (Fusion)
Security	8	9	10
Performance	10	6	8
Key Size	9	5	8
Energy Efficiency	10	5	7
Implementation Complexity	7	8	9

Table 1: Evaluation of Encryption Algorithms Based on Key Metrics

5.3 Comparison of AES, RSA, and AES+RSA (Fusion) Across Key Metrics



Graph 1: Evaluating Security, Performance, and Efficiency of Encryption Methods

The graph compares AES, RSA, and their fusion (AES+RSA) across five key metrics: Security, Performance, Key Size, Energy Efficiency, and Implementation Complexity. AES scores highest in performance and efficiency, while RSA excels in security but lags in other areas due to high resource demands. The fusion method (AES+RSA) balances strengths, achieving robust security with reasonable performance and efficiency, making it ideal for scenarios demanding both encryption speed and secure key exchange.

VI. CONCLUSION

The hybrid AES+RSA encryption model provides an optimal solution for securing XR environments by combining the strengths of both AES and RSA encryption techniques. AES ensures fast and efficient data encryption, while RSA handles secure key exchange, providing robust protection for transmitted data. The dual-key system ensures both confidentiality and integrity, with RSA encrypting the symmetric AES session key and AES encrypting the XR data.

The architecture consists of three layers: input, processing, and output, which securely manage real-time data and multimedia content. The AES+RSA fusion balances high security with reasonable performance and efficiency, making it ideal for applications that require both fast encryption and secure key management.

REFERENCES

1. Ahmed, A., & Khan, M. (2023). Performance and security of AES, DES, and RSA in hybrid systems. International Journal of Computer Engineering and Security, 10(2), 55-60. Retrieved from ijcesen.com
2. Sharma, V., & Gupta, R. (2023). RSA and AES based hybrid encryption technique for enhancing data security in cloud computing. ResearchGate. Retrieved from researchgate.net
3. Verma, S., & Yadav, P. (2024). A hybrid approach using AES-RSA encryption for cloud data security. International Journal of Information Security and Applications Engineering, 4(1), 33-40. Retrieved from ijisae.org
4. Singh, A., & Kumar, S. (2023). Hybrid cryptosystem using RSA, DSA, Elgamal, and AES. ResearchGate. Retrieved from researchgate.net
5. Raj, R., & Kumar, A. (2024). Enhancing performance of hybrid AES, RSA, and quantum encryption algorithm. Figshare. Retrieved from aru.figshare.com
6. Gupta, S., & Singh, P. (2023). AES-RSA: An innovative hybrid security framework for file storage. International Journal of Information Security and Applications Engineering, 4(2), 55-63. Retrieved from ijisae.org
7. Patel, M., & Shah, K. (2024). Secure file storage on cloud using AES, RC6, and Blowfish algorithm. International Journal of Advanced Research in Science and Computing Technology, 5(3), 40-48. Retrieved from ijarsct.co.in
8. Thakur, A., & Jain, R. (2023). RSA-AES hybrid encryption: Combining the strengths of two algorithms. International Journal of Research and Review, 11(6), 123-130. Retrieved from ijrar.org
9. Singh, A., & Gupta, P. (2023). Hybrid cryptosystem using RSA, DSA, Elgamal, and AES. ResearchGate. Retrieved from researchgate.net
10. Sharma, V., & Mehta, R. (2023). Performance and security of AES, DES, and RSA in hybrid systems: An empirical analysis of triple encryption. International Journal of Computer Engineering and Security, 9(4), 45-50. Retrieved from ijcesen.com

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details