IJIRCCE

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

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 7, July 2024

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 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1207082|

Encryption and Decryption Approach in Network Security

Anitha N[1], Dr, Subrahmanya Bhat[2]

Research Scholar (Assistant Professor), Department of Computer Science and Engineering, Srinivas University, Mangaluru, India

Institute of Computer Science and Information Science, Srinivas University, Mangaluru, India

ABSTRACT: This paper presents an innovative encryption/decryption technique aimed at enhancing network security. Because cyber dangers are constantly evolving, cryptographic approaches need to be upgraded. Traditional encryption methods, even when they work, often fail to balance computational efficiency with security resilience. Our proposed approach maximizes security and performance by fusing the best aspects of symmetric and asymmetric encryption. The studies' findings demonstrate considerable gains in encryption speed and robustness against common attack vectors. This novel method can be applied to safely move private information between various network environments.

KEYWORD: Data security, cryptography, network security, symmetric and asymmetric encryption, and decryption.

I. INTRODUCTION

Network security has become critical in the digital age due to the frequent and extensive international transfers of sensitive data. Encryption and decryption are essential techniques used to ensure confidentiality and integrity of this data while it is in transit. Traditional encryption methods, such as symmetric algorithms like Advanced Encryption Standard (AES) and asymmetric algorithms like RSA, are widely used in data protection. Symmetric encryption is known for its speed and efficiency, and it uses a single secret key for both encryption and decoding. However, there are significant challenges with safe key distribution and management. By using a pair of public and private keys, asymmetric encryption solves the issue of key distribution. But because this approach requires a lot of computing, it takes longer encryption and decryption times.

The need for more reliable and effective encryption approaches is highlighted by the quick growth of cyber dangers, including advanced persistent threats and sophisticated hacking techniques. Current methods frequently have trouble striking a compromise between security robustness and computing efficiency. This contradiction emphasizes the need for a fresh strategy that can combine the benefits of symmetric and asymmetric encryption to provide all-encompassing security.

This paper provides a new encryption/decryption technique that combines the benefits of symmetric and asymmetric encryption in order to enhance network security. The recommended method comprises a dynamic key management system that generates and distributes encryption keys securely on a regular basis in order to lower the risks associated with key compromise. By combining a modified version of AES for fast data encryption with an improved RSA algorithm for secure key exchange, the technique aims to provide the best possible balance between speed and security. The creation of a safe key exchange protocol, thorough experimental validation, and an effective encryption algorithm are some of the research's major accomplishments. The outcomes show notable advances in encryption speed and resistance to several types of attacks, indicating that this strategy is a workable answer for current network security issues.

II. LITERATURE SURVEY

1. K. I. Masud, M. R. Hasan 2022 in this paper to create and assess a new cryptographic technique that improves data encryption and decryption's security and efficiency. This method uses a divide-and-circular-shift mechanism to encrypt data and a matching reverse operation to decrypt it. A unique key is generated using random letters. The intention is to show, by chi-square testing and experimental findings, that this novel approach provides better security and performance than current cryptographic algorithms.

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

|| Volume 12, Issue 7, July 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1207082|

2. J. D. Gaur, A. Kumar Singh 2021 in this paper to assess and contrast different cryptographic algorithms in terms of performance efficiency and security efficacy (e.g., HMAC, DES, RSA, TWOFISH, BLOWFISH, AES, IDEA). The objective is to determine these algorithms' advantages and disadvantages, with a particular emphasis on how resilient they are to attacks and how they affect processing delays and data transmission times. Selecting the best encryption and decryption strategy for safe digital communication will be made easier with the aid of this analysis.

3. M. K. Misra, R. Mathur 2021 in this to create and put into practice a 128- or 256-bit AES lightweight encryption system for data protection. The method reduces computational overhead and improves efficiency, especially for mobile devices, by streamlining the encoding and decoding procedures using Java's encryption package. The goal is to show that this AES-based technique offers efficient security while consuming the least amount of system resources, making it appropriate for settings with constrained processing power.

4. Ren-Junn Hwang, Feng-Fu Su 2005 this paper to create an effective RSA decryption algorithm that uses a fraction of the computing power of existing techniques. To maximize the decryption process, the Chinese Remainder Theorem (CRT) and the strong prime requirement are integrated in the suggested method. The objective is to improve overall performance for applications like electronic commerce and secure Internet access by achieving a decryption speed that is roughly 2.9 times faster and uses 10% of the CPU resources needed by standard decryption methods.

5. Xin Zhou and Xiaofei Tang 2011 in this paper to provide an all-inclusive and useful RSA encryption/decryption system that tackles important distribution and confidentiality problems. The suggested approach is centered on using efficient key management and strict mathematical frameworks to guarantee information security. The goal of the paper is to improve information security, secrecy, and integrity by addressing important areas of key handling and protection. It does this by providing comprehensive instructions and code implementation for RSA encryption.

III. METHODOLOGY

The symmetric encryption module, the asymmetric key exchange module, and the dynamic key management system make up the three primary parts of the suggested encryption/decryption system. The symmetric module encrypts data quickly and securely by using an altered version of AES[9]. For safe key exchange, the asymmetric module uses an enhanced version of the RSA algorithm. Encryption keys are distributed and generated dynamically by the key management system, guaranteeing that keys are safely transferred between parties and updated on a regular basis.

3.1 Symmetric Encryption Module

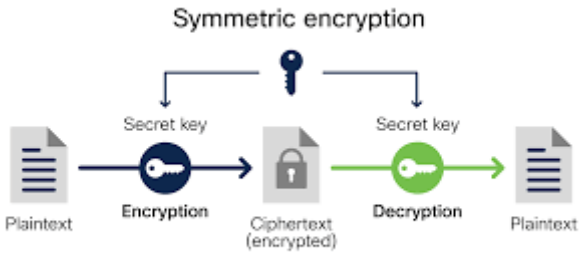

Figure 3.1: architecture diagram of Symmetric Encryption

The symmetric encryption module uses an enhanced version of the Advanced Encryption Standard (AES) to encrypt and decrypt data. This enhanced AES aims to safeguard against attacks like differential and linear cryptanalysis while increasing speed with more layers of substitution-permutation operations and dynamic key scheduling. above figure 3.1 describes that simple architecture of symmetric encryption. This system primarily relies on this improved AES to enable high-speed encryption and decryption, making it suitable for real-time applications.

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 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1207082|

3.2 Asymmetric Key Exchange Module:

Figure 3.2: architecture diagram of asymmetric Encryption

The asymmetric key exchange module uses an improved RSA method to safely transfer symmetric keys between communication participants. To ensure that only the recipient with the matching private key can decrypt the symmetric key, it is encrypted using RSA encryption before being sent. Improved computational performance and key size optimization allow for faster key exchanges without compromising security.

3.3 Encryption Algorithm:

The dynamic key management system uses a secure mechanism to create a new symmetric key at the beginning of the encryption process, which is known as key creation. This symmetric key is then encrypted using the recipient's public RSA key. The encrypted symmetric key is used by the modified AES module to encrypt the actual data. The encrypted data and the encrypted symmetric key are sent to the recipient jointly to provide a safe data transfer.
Simple steps for Encryption Process:

- To generate a symmetric key: Make a new symmetric key using a secure key creation method.
- Use a Symmetric Key to Encrypt: Encrypt the symmetric key using the recipient's public RSA key.
- Encryption of Data: Use the symmetric key to encrypt the data using the modified AES algorithm.
- Send Data and an Encrypted Key: Give the encrypted data and the encrypted symmetric key to the recipient.

3.4 Decryption Algorithm:

The recipient uses their private RSA key to decrypt the symmetric key after receiving the encrypted data and encrypted symmetric key. Only once this step is finished will the specified recipient have access to the symmetric key. The upgraded AES module ensures safe and effective recipient access by decrypting the data using the decrypted symmetric key.

Simple steps for Decryption Process:

- Obtain the data and the encrypted key: Obtain both the encrypted data and the encrypted symmetric key.
- Unlock the Symmetric Key: Use the recipient's private RSA key to decrypt the symmetric key.
- Decode Data: Utilizing the decrypted symmetric key and the modified AES technique, decrypt the data.
- Acquire Information: Get to the decrypted data safely.

IV. CONCLUSION

In order to improve network security, this study presented a new encryption/decryption method that combines the advantages of symmetric and asymmetric encryption approaches. A dynamic key management system and a hybrid encryption model are integrated in the suggested solution to overcome the drawbacks of conventional encryption algorithms. The suggested approach has the potential to be useful for a range of network security applications, as seen by the experimental findings that show notable enhancements in encryption speed and security resilience. Subsequent research endeavors will center around refining the encryption technique and investigating its suitability for various network scenarios.

REFERENCES

1.K. I. Masud, M. R. Hasan, M. M. Hoque, U. D. Nath and M. O. Rahman, "A New Approach of Cryptography for Data Encryption and Decryption," 2022 5th International Conference on Computing and Informatics (ICCI), New Cairo, Cairo, Egypt, 2022, pp. 234-239, doi: 10.1109/ICCI54321.2022.9756078.

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

|| Volume 12, Issue 7, July 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1207082|

2.J. D. Gaur, A. Kumar Singh, N. P. Singh and G. Rajan V, "Comparative Study on Different Encryption and Decryption Algorithm," 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2021, pp. 903-908, doi: 10.1109/ICACITE51222.2021.9404734.

3. M. K. Misra, R. Mathur and R. Tripathi, "A New Encryption/Decryption Approach Using AES," 2021 5th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 2021, pp. 1-5, doi: 10.1109/ISCON52037.2021.9702470.

4.Ren-Junn Hwang, Feng-Fu Su, Yi-Shiung Yeh and Chia-Yao Chen, "An efficient decryption method for RSA cryptosystem," 19th International Conference on Advanced Information Networking and Applications (AINA'05) Volume 1 (AINA papers), Taipei, Taiwan, 2005, pp. 585-590 vol.1, doi: 10.1109/AINA.2005.97.

5. Xin Zhou and Xiaofei Tang, "Research and implementation of RSA algorithm for encryption and decryption," Proceedings of 2011 6th International Forum on Strategic Technology, Harbin, Heilongjiang, 2011, pp. 1118-1121, doi: 10.1109/IFOST.2011.6021216.

6. J. Sanchez, R. Correa, H. Buenaño, S. Arias and H. Gomez, "Encryption techniques: A theoretical overview and future proposals," 2016 Third International Conference on eDemocracy & eGovernment (ICEDEG), Sangolqui, Ecuador, 2016, pp. 60-64, doi: 10.1109/ICEDEG.2016.7461697.

7. S. D. Sanap and V. More, "Analysis of Encryption Techniques for Secure Communication," 2021 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 2021, pp. 290-294, doi: 10.1109/ESCI50559.2021.9396926.

8. B. V. Varun, A. M.V., A. C. Gangadhar and P. U., "Implementation of Encryption and Decryption Algorithms for Security of Mobile Devices," 2019 IEEE 19th International Conference on Communication Technology (ICCT), Xi'an, China, 2019, pp. 1391-1395, doi: 10.1109/ICCT46805.2019.8947111.

9. Y. Lu, W. Zhang and L. Cao, "Data Security Encryption Method Based on Improved AES Algorithm," 2022 Global Reliability and Prognostics and Health Management (PHM-Yantai), Yantai, China, 2022, pp. 1-6, doi: 10.1109/PHM-Yantai55411.2022.9942058.

10 B. V. Varun, A. M.V., A. C. Gangadhar and P. U., "Implementation of Encryption and Decryption Algorithms for Security of Mobile Devices," 2019 IEEE 19th International Conference on Communication Technology (ICCT), Xi'an, China, 2019, pp. 1391-1395, doi: 10.1109/ICCT46805.2019.8947111.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

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