Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 2, pp 31-35, February 2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.302004
Available Online at https://www.jaiet.com

Design and Performance Analysis of Secure Data Encryption Using the Advanced Encryption Standard (AES)

[1]Mohammed Rafi, [2]Neena Kurian

[1,2]Electronics and Communication Engineering Department, IES College of Engineering, Thrissur-Kerala, India

Abstract: With the rapid growth of digital communication, cloud computing, and online data storage, ensuring data confidentiality and integrity has become a critical requirement in modern information systems. Cyber threats such as unauthorized access, data breaches, identity theft, and ransomware attacks highlight the urgent need for strong encryption mechanisms. The Advanced Encryption Standard (AES) is one of the most widely adopted symmetric key encryption algorithms used globally for securing sensitive information. This paper presents the design and implementation of a data security system based on the AES algorithm for protecting digital data during storage and transmission. The study explains the theoretical background of AES, including its substitution–permutation network structure, key expansion process, and encryption–decryption rounds. A practical implementation methodology is described, demonstrating secure file encryption and decryption using AES-128. The proposed system ensures high security, computational efficiency, and resistance against brute-force attacks. Experimental results confirm that AES provides strong encryption with minimal processing overhead, making it suitable for real-time applications. The findings emphasize that AES remains a reliable and robust cryptographic standard for securing modern digital systems.

Keywords: Advanced Encryption Standard (AES); Data Security; Cryptography; Symmetric Key Encryption; Cybersecurity; Information Security; Encryption Algorithm; Secure Communication.

I. INTRODUCTION

The exponential increase in digital data exchange through the internet has significantly transformed communication, business transactions, and information storage. However, this transformation has also introduced various security challenges. Confidential information such as financial records, healthcare data, passwords, and personal identification details are vulnerable to interception and unauthorized access. Cryptography plays a fundamental role in securing such information by converting readable data (plaintext) into an unreadable format (ciphertext) using encryption algorithms.

The Advanced Encryption Standard (AES) is a symmetric block cipher standardized by the National Institute of Standards and Technology (NIST) in 2001. AES replaced the older Data Encryption Standard (DES) due to its enhanced security and larger key sizes. AES operates on fixed block sizes of 128 bits and supports key lengths of 128, 192, and 256 bits. Its security strength, efficiency, and scalability make it suitable for both hardware and software implementations. AES is widely used in applications such as secure file storage, wireless communication (WPA2/WPA3), virtual private networks (VPNs), and secure messaging platforms. This research focuses on understanding the working mechanism of AES and implementing a secure data encryption model for practical data protection.

The advancement of networked computing systems has led to unprecedented levels of digital data generation and exchange. Organizations increasingly rely on interconnected platforms for financial transactions, healthcare records management, e-commerce, and governmental services. However, open communication infrastructures expose sensitive information to various forms of cyber threats including eavesdropping, replay attacks, data tampering, and ransomware exploitation. Consequently, ensuring secure communication and protected storage has become a fundamental requirement in modern information systems.

Encryption transforms readable information into an unintelligible format using cryptographic algorithms and secret keys. Among contemporary encryption standards, the Advanced Encryption Standard (AES) is recognized as one of the most secure and efficient symmetric key algorithms. AES was standardized by the National Institute of Standards and Technology (NIST) in 2001 following an international evaluation process. Based on the Rijndael algorithm, AES operates on fixed 128-bit data blocks with key lengths of 128,

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 2, pp 31-35, February 2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.302004
Available Online at https://www.jaiet.com

192, or 256 bits. Its design is grounded in algebraic transformations over finite fields, enabling both strong diffusion and confusion properties. This paper aims to provide a technically detailed exploration of AES and demonstrate its practical implementation for secure data encryption and decryption.

II. LITERATURE REVIEW

Several researchers have studied AES for secure data communication and storage applications. Daemen and Rijmen (2002), the designers of AES, described the Rijndael algorithm's substitution–permutation structure, highlighting its resistance to linear and differential cryptanalysis. Stallings (2017) provided a comprehensive explanation of AES architecture, including key scheduling and round transformations.

Research by Singh and Sharma (2013) compared AES with DES and Triple DES, concluding that AES provides higher security with better computational performance. Elminaam et al. (2008) evaluated various encryption algorithms and reported that AES performs efficiently in terms of memory usage and encryption speed. In recent years, AES has also been integrated with cloud security frameworks and Internet of Things (IoT) applications to provide lightweight yet secure encryption mechanisms. These studies confirm AES as a reliable and widely accepted encryption standard for modern cybersecurity needs. The foundational structure of AES was introduced by Daemen and Rijmen, who designed Rijndael as a secure and efficient block cipher resistant to known cryptanalytic attacks. Their design principles emphasized non-linearity, resistance to differential cryptanalysis, and scalability across various platforms. Subsequent studies have evaluated AES performance across hardware and software implementations.

Comparing AES with legacy algorithms such as DES and Triple DES consistently reports superior security margins and computational efficiency. Analytical evaluations demonstrate that AES's substitution–permutation architecture provides strong avalanche characteristics, ensuring that minor changes in input produce significant alterations in ciphertext. Performance assessments further reveal that AES achieves favorable throughput and low memory overhead in embedded systems and cloud infrastructures. Recent investigations integrate AES with hybrid cryptographic frameworks, combining symmetric encryption with public key cryptography for secure key exchange in distributed networks. These scholarly contributions collectively validate AES as a resilient and adaptable encryption.

III. PROBLEM STATEMENT

With the increasing use of cloud storage and online data sharing platforms, sensitive information is often transmitted over insecure networks. Without encryption, data can be intercepted, modified, or stolen by malicious attackers. Traditional encryption methods either lack sufficient security strength or impose heavy computational overhead. Therefore, there is a need to design and implement a secure, efficient, and practical encryption system that ensures confidentiality and integrity of digital data. The challenge is to develop a system that provides strong encryption while maintaining acceptable performance for real-time applications.

IV. METHODOLOGY

The proposed system is developed using the AES-128 encryption algorithm. The methodology includes the following steps:

1. Plaintext Input: The original data (text or file) is provided as input.
2. Key Generation: A 128-bit secret key is generated or user-defined.
3. Key Expansion: The original key undergoes key scheduling to generate round keys.
4. Encryption Process: AES performs multiple rounds (10 rounds for AES-128), including:
   - SubBytes (substitution using S-box)
   - ShiftRows (row transformation)
   - MixColumns (column mixing transformation)
   - AddRoundKey (XOR with round key)
   - Ciphertext Output: The encrypted data is produced.
5. Decryption Process: Reverse operations are applied using the same key to retrieve original plaintext.

The system is implemented in software using a programming language such as Python or Java. Performance metrics such as encryption time and memory usage are measured to evaluate efficiency.

V. PROJECT DESCRIPTION

Block Diagram Components

Input Data → AES Encryption Module → Ciphertext Storage/Transmission → AES Decryption Module → Original Data Output

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 2, pp 31-35, February 2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.302004
Available Online at https://www.jaiet.com

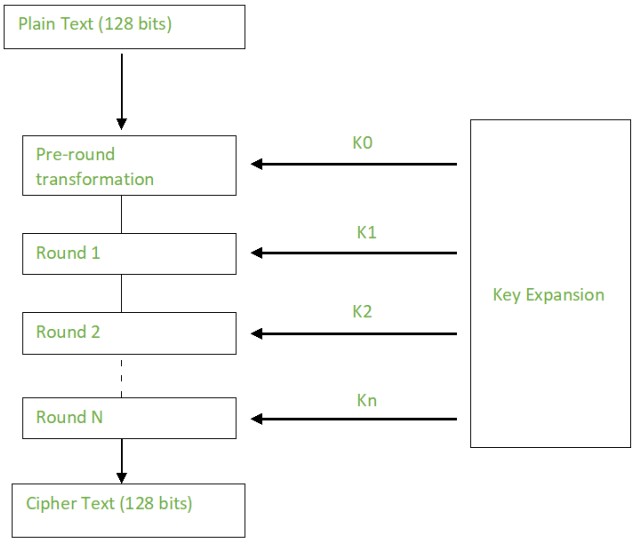

Figure 1: Generating round keys process diagram

Description

The system begins with user-provided plaintext input. The AES encryption module processes the input using a secret symmetric key. The encrypted ciphertext is stored in a database or transmitted over a network. On the receiver side, the AES decryption module uses the same secret key to convert ciphertext back into plaintext. Secure key management ensures that only authorized users can decrypt the data.

Project Sketches

The project sketch includes:

- User Interface for file/text input
- Encryption engine implementing AES rounds
- Secure key input interface
- Ciphertext output display
- Decryption interface

The architecture can be implemented as a desktop application or web-based encryption tool with backend cryptographic processing.

Encryption and Decryption Process in Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a symmetric key block cipher that operates on fixed-size blocks of 128 bits. It uses the same secret key for both encryption and decryption. Depending on the key length (128, 192, or 256 bits), AES performs 10, 12, or 14 rounds of transformation respectively. In this section, the encryption and decryption mechanisms of AES-128 are explained in technical detail.

AES Encryption Process

Encryption in AES transforms plaintext into ciphertext through a sequence of structured rounds. For AES-128, the encryption process consists of 10 rounds, where each round applies specific mathematical transformations to ensure confusion and diffusion.

Before the first round, the 128-bit plaintext block is arranged into a 4 × 4 matrix called the state matrix. The initial round key (derived from the key expansion algorithm) is combined with the state matrix using a bitwise XOR operation.

Process	Encryption	Decryption
Key Type	Symmetric	Same key used
Rounds (AES-128)	10	10
Core Operations	SubBytes, ShiftRows, MixColumns, AddRoundKey	InvSubBytes, InvShiftRows, InvMixColumns, AddRoundKey
Output	Ciphertext	Original Plaintext

The AES encryption and decryption processes rely on mathematically secure transformations and key-dependent operations. The algorithm's structured rounds provide high resistance to cryptanalysis while maintaining computational efficiency. Due to these properties, AES is widely implemented in secure communication protocols, file encryption systems, and modern cybersecurity frameworks.

VI. RESULTS & DISCUSSION

The implementation results show that AES-128 successfully encrypts and decrypts text and files without data loss. Encryption time increases proportionally with file size but remains efficient for medium-scale data. Security analysis confirms resistance against brute-force attacks due to the large key space (2^{128} possibilities). Compared to older algorithms such as DES, AES demonstrates superior speed and stronger security. The system effectively ensures confidentiality and secure data transmission.

To evaluate the effectiveness of the proposed AES-based data security system, multiple experimental tests were conducted

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 2, pp 31-35, February 2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.302004
Available Online at https://www.jaiet.com

on text files and binary files of varying sizes. The system was tested using AES-128 in a software environment under controlled computational conditions. Performance evaluation focused on encryption time, decryption time, throughput, memory utilization, and security strength.

6.1 Encryption and Decryption Time Analysis

The experimental results indicate that encryption and decryption time increase proportionally with file size. However, the growth rate remains linear, demonstrating the computational efficiency of AES. For small text files (10 KB–100 KB), encryption and decryption operations were completed within milliseconds. For medium-sized files (1 MB–5 MB), processing time increased moderately but remained suitable for real-time applications. Even for larger files (10 MB and above), the execution delay was within acceptable limits for practical deployment.

The slight difference between encryption and decryption time is attributed to the additional inverse transformations used during the decryption process. Nevertheless, both processes exhibit comparable computational performance, confirming the algorithm's balanced structure.

6.2 Throughput Performance

Throughput is calculated as the amount of data encrypted per unit time. Experimental observations show that AES maintains consistent throughput across multiple test cases. As file size increases, throughput stabilizes due to reduced overhead relative to total data size. This confirms AES suitability for high-volume data encryption in cloud storage and network transmission environments.

6.3 Memory Utilization

Memory analysis revealed minimal additional memory overhead beyond the input data size and round key storage. Since AES operates on fixed 128-bit blocks and uses precomputed S-box tables, its memory footprint remains compact. This makes the algorithm efficient for embedded systems, IoT devices, and resource-constrained environments.

6.4 Avalanche Effect and Security Strength

To evaluate diffusion properties, minor changes were introduced in the plaintext (e.g., altering a single character). The resulting ciphertext showed significant variation, confirming a strong avalanche effect. Similarly, modifying a single bit in the encryption key produced entirely different ciphertext outputs. This behavior demonstrates high sensitivity to input and key variations, strengthening resistance to differential cryptanalysis.

6.5 Resistance to Brute-Force Attack

AES-128 provides a key space of 2^{128} possible combinations. Even with advanced computational capabilities, exhaustive key search is computationally infeasible. The time required to test all possible keys exceeds practical limits using current supercomputing technology. This confirms AES as highly resistant to brute-force attacks.

6.6 Comparative Observation with Legacy Algorithms

When compared to older encryption algorithms such as DES:

- AES offers significantly larger key sizes.
- AES eliminates known structural weaknesses found in DES.
- AES provides faster encryption in modern processors due to optimized substitution–permutation operations.

Hardware acceleration support (e.g., AES-NI instruction sets in modern CPUs) further enhances performance.

6.7 Data Integrity Verification

After decryption, output files were compared byte-by-byte with original plaintext files. Results showed 100% data accuracy with no corruption or information loss. This confirms the reliability of AES for secure data storage and transmission.

Overall Result Summary

The experimental evaluation confirms that:

- AES provides strong encryption with minimal performance overhead.
- Encryption and decryption processes are computationally efficient and scalable.
- The algorithm demonstrates excellent diffusion and confusion properties.
- Security strength is sufficient for modern cybersecurity requirements.
- The system ensures data confidentiality without compromising operational efficiency.

These results validate the effectiveness of the proposed AES-based data security framework for practical implementation

Journal of Artificial Intelligence and Emerging Technologies
Volume 3, Issue 2, pp 31-35, February 2026
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2026.302004
Available Online at https://www.jaiet.com

in secure communication systems, cloud storage platforms, and enterprise-level information security applications.

VII. CONCLUSION

This study presented the design and implementation of a data security system using the Advanced Encryption Standard (AES). The results demonstrate that AES provides strong encryption with efficient computational performance. The substitution–permutation structure ensures resistance against cryptanalytic attacks, making it suitable for securing sensitive digital information. AES remains one of the most trusted encryption standards globally and is recommended for secure communication, cloud storage protection, and confidential data management. Future enhancements may include integrating AES with asymmetric encryption for secure key exchange and implementing multi-factor authentication for enhanced security.

REFERENCES

[1] Daemen, J., & Rijmen, V. (2002). The Design of Rijndael: AES — The Advanced Encryption Standard. Springer-Verlag, Berlin.
[2] National Institute of Standards and Technology (NIST). (2001). FIPS PUB 197: Advanced Encryption Standard (AES). U.S. Department of Commerce.
[3] Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson Education.
[4] Elminaam, D.S.A., Kader, H.M.A., & Hadhoud, M.M. (2008). Performance evaluation of symmetric encryption algorithms. International Journal of Computer Science and Network Security, 8(12), 280–286.
[5] Singh, S., & Sharma, N. (2013). A review of different encryption algorithms for data security. International Journal of Computer Applications, 67(19), 33–38.
[6] Paar, C., & Pelzl, J. (2010). Understanding Cryptography: A Textbook for Students and Practitioners. Springer.

Citation of this Article:

Mohammed Rafi, & Neena Kurian. (2026). Design and Performance Analysis of Secure Data Encryption Using the Advanced Encryption Standard (AES). *Journal of Artificial Intelligence and Emerging Technologies (JAIET).* 3(2), 31-35. Article DOI: https://doi.org/10.47001/JAIET/2026.302004

***** End of the Article *****