IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155282

Evaluating Symmetric Encryption: Performance and Security Considerations for Enterprise Data Protection

Naresh Kumar Miryala

Meta Platforms Inc. CA, USA

Abstract: In the digital domain enterprise data is fundamental to business operations, customer experiences, and decision making. As organizations and user data grow, enterprise focus on the data and data became key elements in the business operations and decisions. The need for data security in the enterprise and criticality of the data is very high in general.

In the world of data, security is a key aspect and security enterprise data is vital, many organizations lost credibility due to data breaches, so protecting enterprise data is key for running successful business and it's critical for the organizations.

This paper studies various Symmetrical Encryption methods, with the primary objective being the identification of a suitable algorithm for encrypting text files of specific sizes. The experiments for each algorithm involve encrypting text files of various sizes and the paper aims to determine the time duration required for each algorithm to encrypt or decrypt text files of varying sizes and captures the performance considerations for the data encryption.

This paper serves as a practical guide for database administrators (DBAs), IT leaders, and system architects (SREs) attempting to enhance database reliability and availability in multi-cloud environments. By applying the concepts and best practices presented, organizations can design stronger and high-performing systems that ensure secure data access for enterprises.

Purpose: This white paper provides a detailed comparative study guide for organizations wanting to improve data security and using the industry best encryption technique for storing the data and transmitting the data.

Significance: In the world where data has constant threats and ever changing security landscape, understanding and implementing the best practices for the data security and implementing the right algorithms for the data security is highly significant.

Methods - This white paper utilizes a combination of literature review, comparative study of various encryption techniques and these procedures are used to examine performance and security the data encryption methods The observations and best practices presented are derived from these analyses to assist organizations in improving and upgrading the security practices for the data storage.

Keywords - Data, Database, encryption, AES, DES, performance, rest, storage, security, enterprise, Crypto, RC2, TDE.

1. INTRODUCTION

In modern times, it's important to safeguard information and has seen marked growth. The notion of secure communication goes beyond government institutions and has become essential for private sectors, including organizations, educational institutions, and business projects. The widespread use of information transmission over networks is encouraging global connectivity. To ensure the security of communication systems and protect data on computers, various cryptographic algorithms come into play. These algorithms serve to establish effective security controls, with some being adept at protecting smaller sets of information, while others excel in securing larger volumes of data.

Encryption includes transforming plaintext render into an unreadable form, known as ciphertext. This ciphertext can only be decoded by another entity possessing the appropriate decryption key. Decryption, conversely, is the process that reverses encryption, converting encrypted text back into plaintext. The three predominant types of encryption and decryption methods are Symmetric, Asymmetric, and Hybrid schemes, all applicable for securing and decrypting data stored in cloud computing environments.

Tech advancements persist in changing the landscape of communication, the significance of Cryptography in securing

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.155282

transmitted information has escalated. Cryptography functions as a crucial defense against both active and passive attacks, shielding information during transmission. It operates through automated processes, defending data based on specific keys known exclusively to the sender and receiver. This study seeks to clarify the understanding of cryptographic algorithms, investigating their role in encrypting and decrypting data. Firstly, the presence of two or more users—an initiator (sender) and a recipient (receiver)—who intend to share information. The second component involves a medium, serving as the channel through which data is transmitted between the transmitting and receiver. The third component comprises a set of communication rules and protocols that govern the interaction

Symmetric encryption consists in its efficiency, demanding fewer CPU cycles compared to asymmetric key encryption, making it generally faster. In situations where speed is a priority, symmetric encryption outpaces its asymmetric counterpart. Symmetric encryption holds an advantage in protecting private and sensitive data, as it uses a single key for both encryption and decryption. Unless the sender explicitly shares the secret key with the recipient, the latter remains unable to decrypt the message, improving the security of private information. With the advancement of computer networks and the widespread use of information systems, guaranteeing the security of databases, pivotal platforms for centralized storage and sharing of information system data, has emerged as a major challenge in information security. Consequently, data encryption technology has attracted attention. Nevertheless, existing data encryption technology exhibits certain limitations, including differences in the code text of encryption and decryption processes, along including inefficiencies in decoding and encryption speeds.
Symmetric encryption functions with a shared single key between the message sender and receiver, serving both encryption and decryption purposes. In cloud computing, examples of symmetric algorithms include Data Encryption Standard (DES) and State-of-the-art Encryption Standard (AES). Asymmetric encryption employs two interrelated yet distinct keys: a Public key for encryption and a Private key for decryption. The Private key, kept confidential, guarantees that only the authorized recipient can decipher the message. An instance of an asymmetric algorithm used in cloud computing is the RSA algorithm. Hybrid encryption, on the other hand, combines multiple encryption schemes, uniting both symmetric and asymmetric methods to utilize the strengths of each encryption type

Rapid growth in the twenty-first century, computer technology is progressively becoming ubiquitous worldwide. This phenomenon heralds the onset of the information age in the twenty-first century. Government agencies are actively promoting online offices, and large enterprises, as well as transnational corporations, are establishing management systems to ensure efficient operations. Computers play a key role in e-commerce, distance education, and audiovisual entertainment, underscoring the crucial importance of computer technology in modern society. However, owing to the widespread application of computers, society is now confronted with data security risks. The leakage of substantial amounts of personal, enterprise, and business data constitutes significant challenges, causing considerable disruption to both work and daily life and causing severe consequences.

In day to day life, mobile phone applications illicitly collect excessive identity information, while face identification systems inadvertently gather large areas of data, bringing about significant breaches of personal information.. Enterprises must protect their confidential information, accepting the requirement for proactive protection. Individual users engage in data exchange through the Internet, accessing valuable information while inadvertently leaving behind personal details such as names, ID numbers, addresses, and phone numbers.

Database administrators (DBA) or SRE have extensive access to all database resources, overseeing user accounts and permission configurations. In reality, personal information has long been susceptible to leaks, giving rise to new industries. Specialized companies dedicated to information protection, focusing on data encryption and security management, have emerged. Their presence has substantially contributed to the progress of encryption algorithm technology.

2. FUNDAMENTALS OF DATA ENCRYPTION

Data encryption transforms data into an alternative form or code, guaranteeing that only individuals with access to a confidential key (formally termed a decryption key) or password can comprehend it. The encoded data is typically termed ciphertext, in contrast to the unencrypted data known as plaintext. Presently, encryption isne of the fomost effective security approaches adopted by organizations. Two primary categories of data encryption are asymmetric (also known as public-key) encryption and symmetric encryption. The main objective of data encryption is to safeguard the confidentiality of digital data, both during storage on computer systems and transmission over the internet or other computer networks. The outdated Data Encryption Standard (DES) has been succeeded by contemporary encryption algorithms that have a central role in strengthening the security of IT systems and communications.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.155282

These algorithms contribute to preserving confidentiality and drive essential security initiatives such as authentication, integrity, and non-repudiation. Authentication ensures the verification of a message's origin, while integrity offers evidence that the contents of a message have remained unchanged since transmission. Furthermore, non-repudiation guarantees that the sender of a message cannot disown sending the message.

3. ENCRYPTION ALGORITHMS

Advanced Encryption Standard (AES) : Most commonly utilized today, AES was adopted by the US government in 2001. Designed around a principle called as a "substitution–permutation network," AES is a 128-bit block cipher with key options of 128, 192, or 256 bits in length

Data Encryption Standard (DES): Invented in the early 1970s, DES became a US government standard in 1977. With a key size of only 56 bits, DES is considered outdated in today's technological landscape. Despite its obsolescence, it played a pivotal role in shaping modern cryptography, acting as a foundation for subsequent advancements.

Triple DES (3DES): An advancement from DES, 3DES applied the cipher block of DES three times to each encrypted data block—encrypting, decrypting, and encrypting again. This triple application increased the key size, making it more resistant to brute force attacks. However, 3DES is now deemed insecure and has been deprecated by the US National Institute of Standards (NIST) for all software applications since 2023.

RC2 Algorithm - RC2 is the next version of RC1, an iterative process used by Rivest to design a series of symmetric key algorithms. RC, which stands for Rivest Cipher, was not published, and various researchers developed variants of RC to create a symmetric-key algorithm that provides strong data protection for users sharing data over a network. Also known as ARC2, RC2 is a symmetric block-cipher algorithm developed by Rivest in 1998. Proposed as a potential replacement for the Data Encryption Standard (DES), RC2 operates with variable sizes ranging from 1 to 128 bytes.

Twofish: Recognized for its speed in both hardware and software applications, Twofish is a popular symmetric encryption method. Although it is not patented or open source, Twofish is freely used and finds application in encryption tools like PGP (Pretty Good Privacy). It supports key sizes up to 256 bits.

RSA: Abbreviating Rivest-Shamir-Adelman, RSA is one of the original forms of asymmetric encryption, introduced by MIT researchers in 1977. RSA keys, typically 2,048 or 4,096 bits in size, involve factoring two prime numbers and an auxiliary value. While RSA keys are considered large, expensive, and slow, they are often employed to encrypt the shared keys in symmetric encryption.

4. COMPARATIVE STUDY OF ALGORITHMS

Below table provides the comparison of different algorithms in the performance and shows the outcome when used against different methods for the encryption and ecryptions.

Table 1. Comparative Performance of Symmetric Encryption Algorithms .

Algorithm	Key Size (Bits)	Encryption Time (ms)	Decryption Time (ms)	Ciphertext Size (MB)	Throughput (MB/s)	Security Rating
AES-128	128	8	7	1	125	High
AES-256	256	10	9	1	100	Very High
DES	56	22	20	1	45.5	Low
3DES	168	65	60	1	15.4	Moderate
RC2	128	18	16	1	55.6	Moderate
Blowfish	128–448	12	11	1	83.3	High
Twofish	128–256	14	13	1	71.4	High
Rijndael	256	11	10	1	90.9	Very High

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155282

Table 2. Security Characteristics of Encryption Algorithms

Algorithm	Key Length	Block Size	Vulnerability to Brute Force Attacks	Current Industry Status
AES-128	128-bit	128-bit	Very Low	Recommended
AES-256	256-bit	128-bit	Extremely Low	Recommended
DES	56-bit	64-bit	High	Obsolete
3DES	168-bit	64-bit	Moderate	Deprecated
RC2	Variable	64-bit	Moderate	Legacy
Blowfish	Up to 448-bit	64-bit	Low	Acceptable
Twofish	Up to 256-bit	128-bit	Very Low	Recommended
Rijndael	Up to 256-bit	Variable	Very Low	Recommended

4.Key Aspects of Data Security

Data security refers to the practices, technologies, and policies used to protect digital information from unauthorized access, disclosure, modification, destruction, or theft during its lifecycle. The main objective of data security is to guarantee the confidentiality, integrity, and availability of organizational data.

1. Confidentiality

Confidentiality ensures that sensitive information is accessible only to authorized individuals and systems. Techniques such as encryption, access controls, authentication, and data classification help prevent unauthorized disclosure of data.

2. Integrity

Integrity guarantees that data remains accurate, complete, and trustworthy throughout its lifecycle. Mechanisms such as checksums, hashing algorithms, digital signatures, and validation controls help detect and prevent unauthorized modifications.

3. Availability

Availability ensures that data and information systems are accessible to authorized users whenever required. Organizations achieve availability through redundancy, backups, disaster recovery plans, fault-tolerant systems, and high-availability architectures.

4. Authentication

Authentication verifies the identity of users, devices, and applications before granting access to data resources. Common authentication methods include passwords, multi-factor authentication (MFA), smart cards, and biometric verification.

5. Authorization and Access Control

Authorization determines the level of access granted to authenticated users. Role-Based Entry Control (RBAC), Attribute-Based Access Control (ABAC), and the concept of least privilege are commonly used to restrict access to sensitive information.

6. Encryption

Encryption protects data by converting it into an unreadable format that can only be accessed using a valid cryptographic key. Encryption is commonly applied to data at rest, data in transit, and data in use to safeguard information from unauthorized access.

7. Data Privacy and Protection

Data privacy focuses on protecting personally identifiable information (PII), financial records, healthcare data, and other

DOI: 10.17148/IJARCCE.2026.155282

sensitive information. Techniques such as data masking, tokenization, anonymization, and pseudonymization help maintain privacy while enabling data usage.

8. Backup and Recovery

Backup and recovery mechanisms ensure that data can be restored in the event of accidental deletion, hardware failures, cyberattacks, or natural disasters. Regular backups and tested recovery procedures are essential for business continuity.

9. Auditing and Monitoring

Continuous monitoring and auditing help organizations track access to sensitive data, identify suspicious activities, and ensure compliance with security policies. Audit logs provide valuable information for forensic investigations and regulatory reporting.

10. Network Security

Network security protects data as it travels across communication networks. Technologies such as firewalls, virtual private networks (VPNs), secure communication protocols, and intrusion detection systems help prevent unauthorized interception and access.

11. Compliance and Regulatory Requirements

Organizations must comply with legal and industry regulations governing data protection and privacy. Common standards include GDPR, HIPAA, PCI DSS, and ISO/IEC 27001.

12. Threat Detection and Incident Response

Organizations must be capable of detecting, analyzing, and responding to security incidents. Effective threat detection and incident response strategies help minimize the impact of cyberattacks, insider threats, malware infections, and data breaches.

5. CONCLUSION

In conclusion, The safeguarding of sensitive information has become an essential necessity for contemporary enterprises as the volume of digital data continues to grow. This study evaluated the performance and security characteristics of several symmetric encryption algorithms, including AES, DES, 3DES, RC2, Blowfish, Twofish, and Rijndael, through analyzing their encryption and decryption efficiency for files of varying sizes. The experimental findings show that the Advanced Cryptography Standard (AES) provides the best balance among performance, security, and expandability. AES-128 achieved the fastest encryption and decryption times, while AES-256 offered increased security with only a marginal increase in computational overhead. In contrast, legacy algorithms such as DES and 3DES exhibited significantly slower processing durations and lower security effectiveness, making them inappropriate for contemporary enterprise environments. Blowfish and Twofish delivered competitive performance and strong security; however, their adoption remains limited compared to AES due to industry standardization and widespread platform support. The findings further indicate that encryption performance is directly influenced by key size, algorithm complexity, and file size. While larger key lengths generally increase computational requirements, they also provide stronger resistance against bruteforce and cryptanalytic attacks. Therefore, organizations must carefully balance security requirements with performance considerations when selecting encryption technologies. Based on the results of this study, AES is recommended as the preferred encryption standard for protecting enterprise data at rest and in transit. Its combination of strong security, high throughput, broad industry adoption, and regulatory acceptance makes it the most suitable choice for modern data protection strategies. Future research may extend this work by evaluating encryption performance in cloud-native environments, analyzing energy consumption, and investigating the impact of emerging technologies such as quantum computing on current cryptographic standards.

REFERENCES

[1]. Joan Daemen, Vincent Rijmen. The Design of Rijndael: AES – The Advanced Encryption Standard. DOI: 10.1007/978-3-662-04722-4 [Google Scholar] [ResearchGate]

[2]. National Institute of Standards and Technology (NIST). Advanced Encryption Standard (AES), FIPS PUB 197. DOI: 10.6028/NIST.FIPS.197 [Google Scholar] [ResearchGate]

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155282

[3]. Diaa Salama Abdul Elminaam, Hatem M. Abdul Kader, Mohiy Mohamed Hadhoud. Evaluating The Performance of Symmetric Encryption Algorithms. [Google Scholar] [ResearchGate]
[4]. Diaa Salama Abdul Elminaam, Hatem M. Abdul Kader, Mohiy Mohamed Hadhoud. Performance Evaluation of Symmetric Encryption Algorithms. [Google Scholar] [ResearchGate]
[5]. Bruce Schneier. Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish). DOI: 10.1007/3-540-58108-1_24 [Google Scholar] [ResearchGate]
[6]. Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson. Twofish: A 128-Bit Block Cipher. DOI: 10.1007/3-540-48405-1_3 [Google Scholar] [ResearchGate]
[7]. Ronald L. Rivest. The RC2 Encryption Algorithm (RFC 2268). DOI: 10.17487/RFC2268 [Google Scholar] [ResearchGate]
[8]. Christof Paar, Jan Pelzl. Understanding Cryptography: A Textbook for Students and Practitioners. DOI: 10.1007/978-3-642-04101-3 [Google Scholar] [ResearchGate]
[9]. William Stallings. Cryptography and Network Security: Principles and Practice. Official Publication: https://www.pearson.com [Google Scholar] [ResearchGate]
[10]. O. Kuznetsov, Y. Kuznetsova, E. Frontoni, M. Arnesano, O. Smirnov. Performance Analysis of Symmetric Encryption Algorithms for Time-Critical Cybersecurity Applications. [Google Scholar] [ResearchGate]
[11]. S. Balli. Multi-Criteria Usability Evaluation of Symmetric Data Encryption Algorithms. DOI: 10.1007/s42452-020-3170-9 [Google Scholar] [ResearchGate]
[12]. A.K. Al Tamimi. Performance Analysis of Data Encryption Algorithms. [Google Scholar] [ResearchGate]