International Journal of Engineering Research & Science (IJOER) ISSN: [2395-6992] [Vol-12, Issue-3, March 2026]

# A Comparative Study of Encryption Algorithms for Enhancing Data Security in Cloud Computing

Prof. Krutika Vartak[1*]; Mayur Mohite[2]; Shubham Nachnekar[3]

Department of MCA, University of Mumbai, Mumbai, India
*Corresponding Author

***Abstract—*** *Cloud computing provides highly flexible and cost-effective storage solutions for data. However, ensuring storage security remains a challenging task. Encryption methods play a significant role in maintaining the safety of sensitive information stored within cloud systems. This research presents a comparative analysis of three commonly applied encryption algorithms: Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Rivest-Shamir-Adleman (RSA) for evaluating their applicability in protecting cloud-stored information from unauthorized access. The comparison is based on parameters including security strength, key length, and processing speed. The analysis reveals that AES is highly suitable for secure storage due to its low processing cost. RSA is very effective for secure key transfers. In contrast, DES appears inappropriate for secure cloud storage due to its poor security standards.*

***Keywords— AES, Cloud Computing, Data Security, DES, RSA.***

## I. INTRODUCTION

Cloud computing facilitates flexibility and scalability in accessing computing resources, making it a critical platform for data storage and processing. However, storing sensitive data within cloud platforms generates serious security issues, particularly concerning data confidentiality and unauthorized access. Securing data storage remains one of the critical challenges in cloud computing.

Encryption is one of the most effective ways of securing information stored in the cloud. Encryption encodes information into encrypted versions so that only authorized persons can access it. Different types of encryption algorithms include Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Rivest-Shamir-Adleman (RSA). AES is a symmetric encryption algorithm known for its robustness and efficiency. DES is an older algorithm with key-size limitations that make it insecure. RSA is an asymmetric encryption algorithm known for secure authentication and key exchange but entails greater computational expense. Due to variations in security strength and speed, selecting the most effective encryption algorithm for cloud applications remains a vital issue. This paper presents a comparative analysis of AES, DES, and RSA algorithms concerning their efficacy in enhancing data security in cloud computing scenarios.

**Figure 1: Secure Cloud Data Storage Using Encryption**

## II. LITERATURE REVIEW

**TABLE 1**
**SUMMARY OF LITERATURE REVIEW ON ENCRYPTION ALGORITHMS FOR CLOUD SECURITY**

| Reference | Key Findings | Conclusion |
|---|---|---|
| Patel & Patel (2018) | AES performs faster and provides stronger security than DES and RSA | AES is suitable for cloud data encryption |
| Singh & Sharma (2019) | DES is vulnerable due to small key size; AES is more secure | DES is obsolete; AES is preferred |
| Kumar et al. (2019) | RSA ensures secure key exchange but has high computational cost | AES is efficient for data, RSA for keys |
| Albugmi et al. (2019) | AES is widely used in cloud security frameworks | AES balances performance and security |
| Verma & Tripathi (2020) | DES is faster but insecure; AES performs optimally | AES is best for cloud environments |
| Namasudra et al. (2020) | AES uses less CPU and memory than RSA | AES is efficient for cloud storage |
| Jain et al. (2020) | AES shows lowest encryption and decryption time | AES suits large cloud datasets |
| Kaur & Kinger (2021) | DES fails modern security requirements | DES should not be used in cloud systems |
| Malik et al. (2022) | AES outperforms RSA in speed and resource usage | AES is practical for cloud encryption |
| Sharma & Gupta (2022) | Hybrid AES–RSA improves security and efficiency | AES–RSA hybrid enhances cloud security |
| NIST (2001) | AES standardized for strong encryption | AES is a global encryption standard |
| Stallings (2017) | AES is stronger than DES; RSA used for secure exchange | Modern systems should use AES |
| Bhatia & Khurana (2021) | AES ensures better confidentiality in cloud | AES is recommended for cloud storage |
| Choudhary & Pateriya (2021) | RSA has high overhead for large data | RSA is unsuitable for bulk encryption |

## III. ENCRYPTION ALGORITHMS OVERVIEW

Encryption algorithms play a key role in maintaining data confidentiality in cloud computing. This research examines three popular algorithms: AES, DES, and RSA.

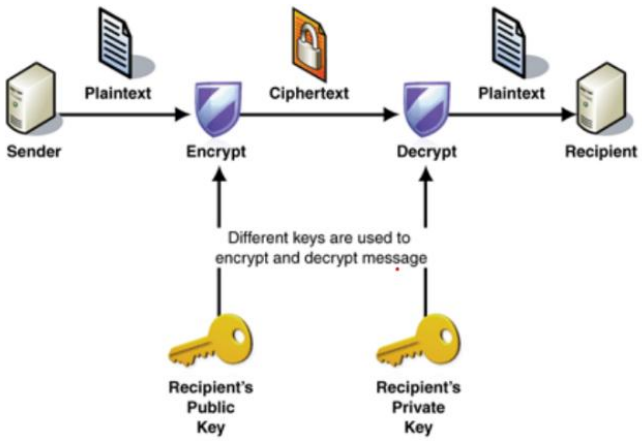


**Figure 2: Public Key Cryptography Encryption and Decryption Workflow**

### 3.1 Advanced Encryption Standard (AES)

AES provides symmetric encryption with high levels of security and performance. It supports key lengths of 128, 192, and 256 bits and is most commonly used for encrypting bulk data in cloud technology.

### 3.2 Data Encryption Standard (DES)

DES is a symmetric key cryptographic technique with a key strength of 56 bits. Due to its vulnerability to security attacks and brute-force attacks, DES is not recommended for cloud environments.

### 3.3 Rivest–Shamir–Adleman (RSA)

RSA is an asymmetric encryption technique largely utilized for secure key exchange and authentication. However, despite being highly secure, it is inefficient for encrypting bulk data due to its high computational costs.

## IV. PROBLEM DEFINITION

Cloud computing has transformed data storage and processing with its scalable, flexible, and cost-effective services. However, storing sensitive information in cloud environments exposes data to various security threats, including unauthorized access, data breaches, and cyber-attacks. Ensuring data confidentiality and integrity within cloud storage remains a critical challenge.

Although many encryption algorithms have been developed to protect cloud data, the features of each algorithm differ. AES, DES, and RSA are among the most popular algorithms widely utilized. AES is efficient and secure for bulk data encryption, DES is faster but insecure due to its smaller key size, and RSA provides high security for key management but is computationally expensive for larger data.

The main problem is to identify which encryption algorithm, or combination of algorithms, provides the best security and performance in cloud computing. A systematic comparative study is necessary to assess these algorithms under similar conditions, considering factors such as encryption/decryption time, computational efficiency, key size, and security strength.

## V. OBJECTIVES OF RESEARCH

The primary aim of this research is to assess and compare the performance and security capabilities of AES, DES, and RSA encryption algorithms in a cloud computing setting and evaluate their applicability for safeguarding cloud-stored data.

The specific objectives are:

1. To assess the speed of AES, DES, and RSA when encrypting and decrypting data of varying sizes
2. To study the key length of the algorithms for their resistance to attack and cryptographic robustness
3. To compare the efficiency and resource usage of algorithms in a cloud environment
4. To determine the most effective algorithm for improving data confidentiality within cloud computing systems
5. To offer recommendations for secure and efficient encryption methods in cloud storage and processing

## VI. METHODOLOGY

This research uses a comparative analysis approach to assess the efficiency of AES, DES, and RSA encryption algorithms for protecting data within cloud computing infrastructure. A comparison has been made based on performance parameters relevant to cloud computing efficiency.

For the comparison, sample data files of varying sizes were chosen to simulate practical cloud storage scenarios. These data files were encrypted and decrypted using standard implementations of AES, DES, and RSA. Experiments were conducted in a controlled environment to ensure equal conditions for all algorithms.

Performance metrics such as encryption time, decryption time, and computational overhead were measured and recorded for each algorithm. Security aspects were evaluated based on key size, algorithm structure, and resistance to known cryptographic attacks. AES was analyzed using different key sizes (128, 192, 256 bits), while DES and RSA were assessed based on their standard configurations.

The collected data was then compared to analyze variations in performance and security strengths of the selected algorithms.


**Figure 3: Cryptographic Encryption Techniques**

## VII. COMPARATIVE ANALYSIS / RESULTS

### 7.1 Encryption Time Comparison

Encryption time is an important factor in evaluating algorithm efficiency, particularly for large cloud datasets. AES consistently shows the fastest encryption times due to its symmetric structure. DES is slightly faster with small files but becomes inefficient as data size increases. RSA, being asymmetric, takes more time for encryption and is less suitable for bulk data encryption.

**TABLE 2**
**COMPARISON OF ENCRYPTION TIME FOR CRYPTOGRAPHIC ALGORITHMS**

| Algorithm | Encryption Time |
|---|---|
| AES | Fastest |
| DES | Moderate |
| RSA | Slowest |

### 7.2 Decryption Time Comparison

Decryption time affects the responsiveness of cloud services. AES has low decryption time, similar to its encryption speed. DES decryption is faster than AES but insecure. RSA is slower than both and is not suitable for large-scale data.

**TABLE 3**
**COMPARISON OF DECRYPTION TIME FOR CRYPTOGRAPHIC ALGORITHMS**

| Algorithm | Decryption Time |
|---|---|
| AES | Fast |
| DES | Moderate |
| RSA | Slow |

### 7.3 Key Size and Computational Overhead Analysis

AES supports key lengths of 128, 192, and 256 bits, providing high security with low computational overhead. DES supports a key length of 56 bits, making it vulnerable to brute-force attacks, though it has low computational overhead. RSA supports key lengths of 1024–4096 bits and is computationally intensive due to larger processing requirements.

**TABLE 4**
**COMPARISON OF CRYPTOGRAPHIC ALGORITHMS BASED ON KEY SIZE AND COMPUTATIONAL OVERHEAD**

| Algorithm | Key Size | Computational Overhead |
|---|---|---|
| AES | 128/192/256 bits | Low |
| DES | 56 bits | Low |
| RSA | 1024–4096 bits | High |

## VIII. SECURITY STRENGTH EVALUATION

- **AES:** Highly resistant to known attacks and considered very secure for cloud data security
- **DES:** Insecure due to small key size and susceptibility to brute-force attacks
- **RSA:** Very secure for cryptographic key exchange and authentication, but not feasible for bulk data encryption

**TABLE 5**
**SECURITY STRENGTH COMPARISON OF ENCRYPTION ALGORITHMS**

| Algorithm | Security Strength |
|---|---|
| AES | High |
| DES | Low |
| RSA | High (for keys/exchange) |

### 8.1 Summary of Comparative Analysis

- **AES:** Most efficient algorithm for encrypting and decrypting large cloud datasets
- **DES:** Outdated and insecure, though it has low computational requirements
- **RSA:** Useful for secure key exchange and authentication, but inefficient for bulk data encryption

## IX. DISCUSSION

The comparative analysis results clearly show notable differences in the performance and security characteristics of AES, DES, and RSA in cloud computing environments. AES is significantly more efficient, with low encryption/decryption time and minimal computational overhead, making it suitable for large-scale cloud data encryption. DES, while relatively simple and fast, provides insufficient security due to its small key space and susceptibility to brute-force attacks. RSA provides superior security features for authentication and secure key exchange but involves high computational costs, making it inefficient for large-scale cloud data encryption.

Each encryption technique has its own strengths and weaknesses. AES ensures security, scalability, and high performance but requires advanced key management systems. DES ensures low computation costs but is insecure for modern cloud computing. RSA ensures secure communication and key management but is inefficient for massive data.

Based on this analysis, it is recommended that AES be used for encrypting data stored in the cloud, while RSA can be used for key exchange and authentication processes. DES should not be used for securing cloud data due to its security flaws. A combination of AES and RSA can further enhance cloud data security.

## X. CONCLUSION

This research provided a comparative review of AES, DES, and RSA algorithms, focusing on their efficiency for improving data security in cloud computing environments. The results reveal that AES offers a balanced combination of security and speed, making it the most preferable algorithm for encrypting cloud data. RSA is highly secure for key exchange and authentication, though inefficient for encrypting large amounts of data. DES is not suitable for cloud environments because it is vulnerable to cryptographic attacks.

The findings can assist organizations and cloud service providers in selecting appropriate encryption methods for cloud data. The application of AES for data encryption combined with RSA for secure key management can effectively enhance cloud data security.

## XI. FUTURE WORK / SCOPE

Future work can focus on improving encryption methods for increased performance in large-scale cloud environments. Research on hybrid encryption models combining AES and RSA may offer improved security with efficiency. Given recent rapid advancements in quantum computing, future work must also investigate post-quantum cryptographic methods to secure cloud data against quantum attacks.

## ACKNOWLEDGMENT

We would like to express our sincere gratitude to everyone who contributed to the successful completion of this research paper. We are highly thankful to **Dr. Arun Kumar**, Principal of VIVA Institute of Technology, for providing us with the opportunity and necessary institutional support. We also extend our heartfelt appreciation to **Prof. Chandani Patel**, Head of the Department (MCA), for her continuous encouragement and for creating a supportive academic environment. We are grateful to all the faculty members of the MCA department for their valuable guidance and assistance throughout this research.

## CONFLICT OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this research paper. This research was conducted purely for academic and research purposes. The authors have no financial, commercial, or personal relationships that could have influenced the results or interpretation of the findings presented in this study

## REFERENCES

[1] Patel, P., & Patel, R. (2018). A comparative study of data encryption techniques for cloud computing. *International Journal of Computer Applications, 181*(22), 1–6. https://www.ijcaonline.org/archives/volume181/number22/29723-2018916663
[2] Singh, S., & Sharma, P. (2019). A review of symmetric and asymmetric encryption algorithms in cloud computing. *International Journal of Advanced Research in Computer Science, 10*(3), 45–52. https://ijarcs.info/index.php/Ijarcs/article/view/6465
[3] Kumar, A., Gupta, R., & Verma, S. (2019). Performance analysis of AES and RSA encryption algorithms for cloud data security. *International Journal of Engineering Research & Technology, 8*(6), 1–5. https://www.ijert.org/performance-analysis-of-aes-and-rsa-encryption-algorithms-for-cloud-data-security
[4] Albugmi, A., Alassafi, M. O., Walters, R., & Wills, G. (2019). Data security in cloud computing. *Journal of Cloud Computing, 8*, Article 12. https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-019-0123-0
[5] Verma, R., & Tripathi, A. (2020). Performance comparison of DES, AES and RSA for data security in cloud. *International Journal of Computer Science and Information Technologies, 11*(2), 78–85. https://ijcsit.com/docs/Volume%2011/vol11issue02/ijcsit2020110223.pdf
[6] Namasudra, S., Devi, D., & Kadry, S. (2020). Data encryption techniques for cloud storage security. *Journal of Information Security and Applications, 50*, Article 102421. https://www.sciencedirect.com/science/article/pii/S2214212619308974
[7] Jain, A., Gupta, N., & Agrawal, S. (2020). Experimental evaluation of encryption algorithms for cloud data security. *International Journal of Scientific & Technology Research, 9*(4), 123–128. https://www.ijstr.org/final-print/apr2020/Experimental-Evaluation-Of-Encryption-Algorithms-For-Cloud-Data-Security.pdf
[8] Kaur, M., & Kinger, S. (2021). Analysis of cryptographic algorithms for cloud computing security. *International Journal of Computer Trends and Technology, 69*(1), 10–15. https://ijcttjournal.org/Volume69/Issue1/IJCTT-V69I1P104.pdf
[9] Malik, M., Khan, A., & Ahmad, R. (2022). Performance evaluation of encryption algorithms in cloud computing. *Journal of Information Security, 13*(2), 45–60. https://www.scirp.org/journal/paperinformation.aspx?paperid=115533
[10] Sharma, A., & Gupta, P. (2022). Hybrid encryption approach using AES and RSA for cloud data security. *International Journal of Advanced Computer Science and Applications, 13*(5), 210–218. https://thesai.org/Publications/ViewPaper?Volume=13&Issue=5&Code=IJACSA&SerialNo=28
[11] National Institute of Standards and Technology. (2001). *Advanced Encryption Standard (AES)* (FIPS PUB 197). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
[12] Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson Education. https://www.pearson.com/en-in/subject-catalog/p/cryptography-and-network-security/P200000006816.