Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 1, No. 2, January : 2024

A COMPREHENSIVE ANALYSIS AND ASSESSMENT OF CLOUD ENCRYPTION ALGORITHMS

Aaqib Nisar Bhat Ph.D. Research Scholar Rimt, University Punjab INDIA. Email: bhataaqibnisar@gmail.com Orcid: 0000-0003-2044-9035
Rajiv Kumar Professor Rimt, University Punjab INDIA. Email:rajivkumar@rimt.ac.in Orcid: 0000-0001-7522-9078

ABSTRACT
Since cloud computing makes it possible to store and handle enormous volumes of sensitive data, it has become a crucial component of contemporary IT infrastructure. But strong security measures are required because of the inherent hazards involved with keeping data in a shared, distant environment. A key element of cloud security is encryption, and several encryption techniques are used to safeguard data both in transit and at rest. This thorough study article provides an in-depth examination of the most popular cloud encryption algorithms, with a particular emphasis on Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES). This Paper examine the benefits and drawbacks of AES and RSA as well as how well-suited each is for various cloud computing technologies. It also go into key management, security issues, and the actual implementation of these methods. This study offers important insights for cloud service providers, security experts, and researchers looking to improve the security posture of cloud-based systems by critically analyzing the state of the art in cloud encryption.

Keywords: Encryption, Cloud, Data, Decryption, Cipher, Data, Key, Security, Hybrid, Message.

I. INTRODUCTION

Cloud computing has become a key paradigm in the modern information technology environment, revolutionizing the delivery and consumption of computer resources and services. Cloud computing is now the foundation for a wide range of applications, from software as a service (SaaS) to data processing and storage, thanks to its scalability, affordability, and accessibility [1]. Nevertheless, there is an important trade-off associated with moving data and apps to the cloud: strong security measures are required to shield private data from illegal access and security lapses [3].

Information systems security aims to achieve three main goals, which are sometimes referred to as CIAs: availability, integrity, and confidentiality. Protecting data from unwanted access and making sure that private information is kept safe is what confidentiality is all about. Maintaining the quality and dependability of the data while guarding against illegal additions or deletions is the main goal of integrity. The guarantee of availability includes the knowledge that data and other IT resources are available to authorized users at all times, providing continuous and prompt access to vital resources [7].

Encryption is a vital component in protecting cloud settings from cyberattacks and data breaches. Cloud security is a complex problem with many facets. Encrypting data while it's in transit and at rest is essential for maintaining confidentiality, integrity, and authenticity in this age of digital transformation, when data is essential to organizations and enterprises.

This review article explores the field of cloud encryption algorithms, concentrating on the two mainstays of contemporary encryption, Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES). AES and RSA are encryption techniques that are very significant and are commonly used in cloud computing to safeguard data and communications [4][5]. Our goal is to present a thorough grasp of these algorithms, their advantages, and how they might be used in a cloud environment.

II. LITERATURE REVIEW

The literature has generally acknowledged the significance of encryption in protecting data transferred and stored via cloud computing [6]. The way computer resources are accessed and used has changed dramatically as a result of cloud computing, which has several benefits including cost-effectiveness and scalability. However, these advantages come with the difficulty of safeguarding private information against illegal access and security breaches; for this reason, encryption is a crucial part of cloud security [8].

Two of the most widely used encryption algorithms in use today are Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES). The stability and effectiveness of AES, which was first developed by Rijmen and Daemen in 2002, make it a popular option for a variety of cloud encryption applications [9]. Electronic Codebook (ECB), Cipher Block Chaining (CBC), and Galois/Counter Mode (GCM) are three of the encryption modes that AES offers; each is designed to meet certain use cases and specifications.

In contrast, RSA is well-known for its contribution to public key cryptography, which makes digital signatures and safe key exchange possible [10]. The mathematical basis of RSA has demonstrated its durability and is still an essential component in cloud communication security. In cloud contexts, this method is especially well-suited for key management.

Cloud encryption presents both potential and concerns that have been covered in a number of in-depth surveys and research. A survey on mobile cloud computing was done by Dinh et al. [2], who focused on the architecture and application elements of cloud security. The significance of safe cloud computing was highlighted by Ristenpart et al.'s investigation of information loss in third-party compute clouds [8].

Balachandra and Chakravarthy implemented an effective RSA cryptography method, highlighting the significance of optimization in cloud encryption algorithms [10]. These studies highlight how encryption methods must advance and how cloud security is a dynamic field.

Building on these fundamental studies, the review article provided here provides a thorough overview of AES and RSA, their useful use in cloud systems, important management techniques, and security considerations. We want to offer a thorough resource for researchers, practitioners, and cloud service providers to improve the security posture of cloud-based systems by critically analyzing the state of the art in cloud encryption.

III. COMPARATIVE ANALYSIS OF SYMMETRIC ENCRYPTION ALGORITHMS

The Advanced Encryption Standard (AES) stands out among the symmetric encryption algorithms available for cloud security because of its reliable security and effective operation. When compared to alternative symmetric encryption methods, AES shows a number of benefits.

Unlike the now-outdated Data Encryption Standard (DES), AES supports 128, 192, and 256-bit keys and enables flexible key lengths. Its security characteristics are strengthened by this flexibility, which increases its resistance to modern cryptographic attacks. Furthermore, AES performs faster than DES, which is important in contemporary computing environments. Due to its fixed 56-bit key length, DES is no longer suitable for secure communications due to its vulnerability to brute-force assaults.

AES remains better to Triple DES (3DES), which is an improvement above DES. Although 3DES uses DES three times in a cascade to increase security, its performance is not as good as AES's. AES is the recommended option for striking a balance between security and efficiency because 3DES's triple encryption procedure causes it to operate more slowly.

Blowfish is unique among alternatives because of its adjustable key lengths, which range from 32 to 448 bits. Nonetheless, AES continues to be the more popular and safe choice. Despite being considered secure, Blowfish has not gained the same traction as AES, a reflection of the latter's prominence in the industry.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 1, No. 2, January : 2024
Another symmetric encryption technique, called Two-fish, supports key lengths of 128, 192, and 256 bits and is made for high security. Although it provides a speed and security balance, Two-fish is not as popular as AES. The latter is still more prevalent in real-world applications due to its demonstrated security and effectiveness.
Finally, Serpent emphasizes security by supporting key lengths of 128, 192, and 256 bits, much like AES. On the other hand, Serpent operates more slowly than AES. AES is still the go-to option for cloud security because of its proven track record and better performance, even with its sturdy construction.

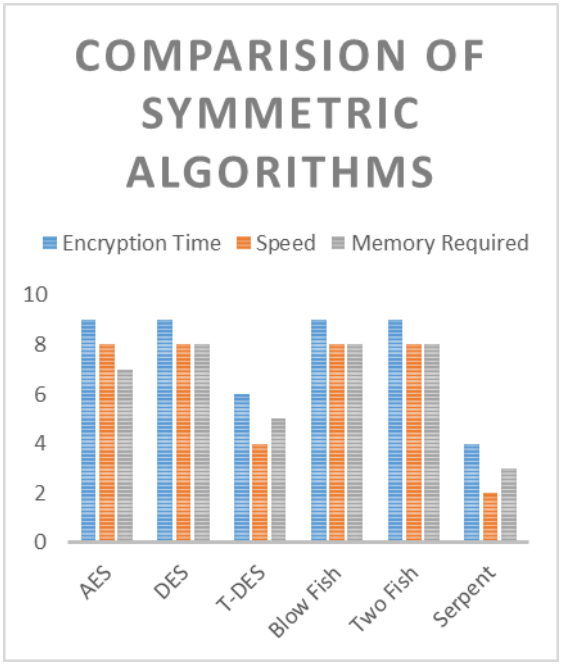

Fig.1 Comparisons of Symmetric Algorithms
The comparative research concludes that AES is the recommended option for many cloud security implementations because it is a flexible and effective symmetric encryption technique. When choosing an algorithm, particular security needs, performance requirements, and industry norms should all be taken into account.

IV. DISCUSSION

A. Strengths and Applications of AES (Advanced Encryption Standard)

One notable example of a strong and effective encryption method that is well-known for its ability to safeguard data in cloud environments is Advanced Encryption Standard (AES). It is appropriate for a variety of cloud use cases due to its adaptability in providing several encryption modes, such as Galois/Counter Mode (GCM), Cipher Block Chaining (CBC), and Electronic Codebook (ECB) [4]. In cloud storage services, AES has become the standard option for encrypting data while it is at rest. Its capacity to protect information with an extreme degree of secrecy while preserving effectiveness makes it an invaluable resource for cloud service providers and consumers.

B. Challenges and Limitations of AES

Even though AES is a well-recognized encryption technique, there are several drawbacks. Key management is one of the main obstacles. It can be difficult to manage encryption keys safely in a cloud setting, and any breach in key security can make encryption ineffective. Furthermore, selecting the right encryption mode is essential since choosing the wrong one might lead to weaknesses, especially in cloud environments with multiple users. To optimize the efficiency of AES in cloud encryption, cloud providers and customers need to carefully examine the recommended methods for key management and mode selection.

C. RSA (Rivest-Shamir-Adleman) for Key Management

In cloud contexts, RSA is essential to key management. It is a useful tool for securely transferring encryption keys between parties due to its asymmetric cryptography features [5]. The authenticity and integrity of data in cloud communications are further improved by the use of RSA in digital signatures. Because of this, RSA is a crucial aspect of many secure cloud applications, especially those that include safe data exchange and multi-tenancy.

D. Performance Considerations:

Due to its influence on reaction times and resource consumption, the cloud encryption algorithms' performance is an important consideration. Most people agree that AES is very effective and appropriate for large-scale cloud installations. Comparing its symmetric encryption model to the asymmetric form of RSA, it requires less computing power. However, key generation and decryption are when RSA's computational cost is most noticeable, which might affect speed in some situations.

V. HYBRID ENCRYPTION AND FUTURE DIRECTIONS

The capabilities of both RSA and AES are combined in hybrid encryption, which is a new development in cloud security. This method makes use of RSA for safe key management and exchange as well as AES for data encryption. When these two techniques are combined, cloud systems' overall security is improved and speed is optimized.

The encryption methods AES and RSA are of utmost significance for cloud security. They are suitable for some areas of cloud encryption and provide clear benefits. AES is the best at encrypting data while it's at rest, but RSA is essential for key management and safe data transfer. A mixture of these algorithms is frequently used in a holistic approach to cloud encryption in order to achieve the ideal balance between security and performance. While choosing and putting encryption algorithms into practice in the cloud, customers and cloud providers alike must take into account their unique security needs and operational limitations. The field of cloud encryption will develop further along with cloud technology, with new algorithms and best practices influencing cloud security in the future.

VI. CONCLUSION

The field of cloud computing is always changing, changing how we handle, store, and use data. Modern information technology now relies heavily on cloud computing due to its cost-effectiveness and scalability. But these advantages come with serious security risks, which is why encryption is essential to cloud security.

This review article has explored cloud encryption techniques, emphasizing Rivest-Shamir-Adleman (RSA) and the Advanced Encryption Standard (AES). These two algorithms, which each shine in different areas, have established themselves as industry leaders in cloud security.

AES is frequently used for data encryption at rest in cloud storage services because of its reputation for robustness and efficiency. Because of its diverse range of encryption mechanisms, it may be used in a variety of scenarios. To properly utilize AES's potential for cloud security, however, efficient key management and mode selection are still essential factors to take into account.

As an asymmetric encryption method, RSA is essential to cloud data interchange and safe key management. Data integrity and authenticity are improved by its usage in digital signatures, especially in multi-tenant cloud systems. For optimal performance, it is important to carefully evaluate the computational complexity of RSA, particularly in key generation and decryption.

The decision between AES and RSA is frequently influenced by the particular operational and security needs of a given cloud situation. A new technique to capitalize on the advantages of both algorithms and strike a balance between security and performance is hybrid encryption, which combines both RSA and AES. The significance of encryption in the dynamic cloud environment cannot be emphasized. To safeguard sensitive data in the cloud, cloud providers, security experts, and researchers

must constantly assess best practices, algorithms, and essential management techniques. New encryption methods and changing recommended practices will continue to influence cloud security as cloud technology develops.

The review study concludes by highlighting the crucial role that encryption algorithms play in cloud computing, using AES and RSA as examples of strong encryption techniques. Because cloud security is dynamic, it requires ongoing research and development to satisfy the changing requirements of cloud providers and consumers. We can successfully manage the challenges of cloud security and take advantage of this game-changing technology if we remain educated and use the best encryption techniques.

Conflict of interest statement

• The authors of this manuscript declare that they have no conflicts of interest related to the research presented in this paper. No financial or personal relationships with other people or organizations have inappropriately influenced this work.

• There is no affiliations with or involvement in any organization or entity with any financial interest such as honoraria, educational grants, participation in speaker's bureaus, membership, employment, or other equity interest.

REFERENCES

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Special Publication 800- 145, 2011.

[2] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," Wireless Communications and Mobile Computing, vol. 13, no. 18, pp. 1587-1611, 2013.

[3] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," in Proceedings of the 16th ACM conference on Computer and communications security, 2009.

[4] V. Rijmen and J. Daemen, "The Design of Rijndael: AES-The Advanced Encryption Standard," Springer, 2002.

[5] M. Balachandra and V. S. Chakravarthy, "An efficient algorithm for RSA cryptography," International Journal of Computer Science and Information Security, vol. 11, no. 6, pp. 17-21, 2013.

[6] R. Kumar and V. Dogra, "Cloud computing: A comprehensive review," Journal of Computer and System Sciences, vol. 84, no. 2, pp. 166-188, 2018.

[7] R. A. Oluoch and N. Masese, "A Review of Emerging Security Issues In Cloud Computing," International Journal of Computer Trends and Technology (IJCTT), vol. 67,no. 9, pp.39-44, 2019.

[8] A. Khajeh-Hosseini, D. Greenwood, and J. W. Smith, "The state of the art in cloud computing," Journal of Research and Practice in Information Technology, vol. 44, no. 1, pp. 1-10, 2012.

[9] V. Rijmen and J. Daemen, "The Design of Rijndael: AES-The Advanced Encryption Standard," Springer, 2002.

[10] M. Balachandra and V. S. Chakravarthy, "An efficient algorithm for RSA cryptography," International Journal of Computer Science and Information Security, vol. 11, no. 6, pp. 17-21, 2013.