Data Encryption in Cloud Storage Using AES and RSA Algorithms

Asha Seshagiri
Software Development Engineer 3 at Expedia, Austin Texas, United States
United States.

DOI: 10.31364/SCIRJ/v12.i08.2024.P0824992
http://dx.doi.org/10.31364/SCIRJ/v12.i08.2024.P0824992

Abstract. This paper discusses data encryption methods in cloud storage using AES and RSA algorithms. The role of these algorithms in ensuring the confidentiality and integrity of data during their storage and transmission through cloud services is analyzed. The advantages of symmetric and asymmetric encryption are discussed, as well as their combined use to improve security and efficiency. In particular, the AES algorithm, based on symmetric encryption, provides high data processing speed, whereas RSA, which is an asymmetric algorithm, provides reliable protection of encryption keys. The work highlights the importance of choosing the right encryption algorithms and methods to ensure data protection in the face of increasing cyber threats and the expansion of the use of cloud technologies.

Keywords: encryption, data encryption, encryption algorithms, cloud storage, AES algorithms, RSA algorithms.

Introduction

The importance of addressing this topic stems from the potential for obtaining confidential information through cyberattacks. For instance, in 2016, Dropbox experienced a cyberattack that compromised 68 million user accounts. The attacker exploited an inadequately protected employee password to gain access to emails and account passwords created before 2012. These data were available for sale on the darknet until the breach was reported by several technology and information outlets.

Despite the convenience of cloud storage, which allows access to information from anywhere in the world at any time and from any device, the security of such storage solutions poses significant concerns for organizations. Storing data in the cloud introduces new types of risks that extend beyond traditional security measures used to protect confidential information in local data centers.

Therefore, organizations must implement additional security measures to protect their data in cloud storage. These measures complement the basic security mechanisms offered by cloud service providers such as Dropbox, Amazon, Microsoft, and Google [1].

This article will explore the specifics of data encryption in cloud storage using AES and RSA algorithms.

General Characteristics of Cloud Storage

Cloud storage offers a convenient way to store information and share files with other users [2]. Cloud encryption platforms ensure the protection of data during its transfer to and from cloud applications, as well as while it is stored on cloud devices. They encrypt data not only during transfer between users and the cloud but also while it is at rest on cloud servers. Such measures prevent unauthorized access and reading of the data.

Cloud storage providers, including AWS, Dropbox, Google Cloud, and Microsoft Azure, offer data encryption at rest. The software used for this purpose automatically handles encryption key exchanges and the processes of encryption and decryption, freeing users from the need to take additional actions beyond authentication and authorization.

The process of implementing and maintaining cloud encryption measures is illustrated in Figure 1.

http://dx.doi.org/10.31364/SCIRJ/v12.i08.2024.P0824992

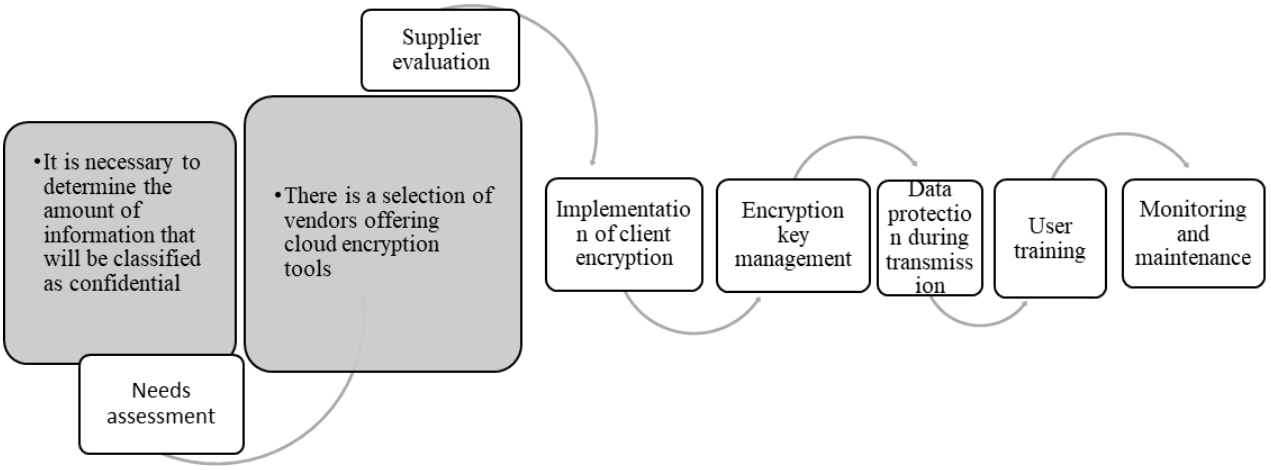

Fig.1. The process of implementing and maintaining cloud encryption measures

Next, we will discuss the reasons why cloud encryption is necessary:

- Protection from unauthorized access: Even if hackers manage to steal data, encryption ensures that without the decryption key, the stolen data remains useless.

- Compliance with industry regulations: Various industries have strict data security regulations. For example, healthcare organizations must comply with HIPAA, while financial companies must adhere to PCI DSS. Encryption helps meet these requirements and avoid penalties.

- Protection of confidential organizational information: Many organizations currently store confidential data in the cloud, such as financial reports, and encryption ensures their protection from unauthorized access.

We will further examine data encryption algorithms in cloud storage, which will be illustrated in Table 1 for clarity.

Table 1. Encryption algorithms

Encryption Algorithm	**Description**
Symmetric Encryption	Uses the same key for both encryption and decryption of data. It is fast and efficient but requires secure key exchange.
Asymmetric Encryption	Involves the use of a pair of keys — public and private. The public key is available to everyone, while the private key is kept secret, ensuring a high level of security.
Hybrid Encryption	Combines symmetric and asymmetric encryption, providing the efficiency of the former and the security of the latter.
End-to-End Encryption	Data is encrypted on the sender's device and can only be decrypted by the receiver's device, ensuring a high level of protection during transmission.
Hashing	Converts data into a fixed-length string of characters (hash), allowing data integrity verification. Although hashing is not encryption in the strict sense, it is often used alongside it to enhance security.

http://dx.doi.org/10.31364/SCIRJ/v12.i08.2024.P0824992

From the presented data, it can be observed that the choice of encryption algorithm depends on specific usage requirements. Hybrid and end-to-end encryption are considered the most secure for cloud storage. However, encryption alone is not sufficient; full data protection also requires implementing access control measures and regular backups [3].

2. AES and RSA Algorithms

The Advanced Encryption Standard (AES) is a symmetric encryption algorithm widely used for data protection. This algorithm is considered highly secure when using a key of proper length, such as 128 or 256 bits. The principle of this algorithm is illustrated in Figure 2.

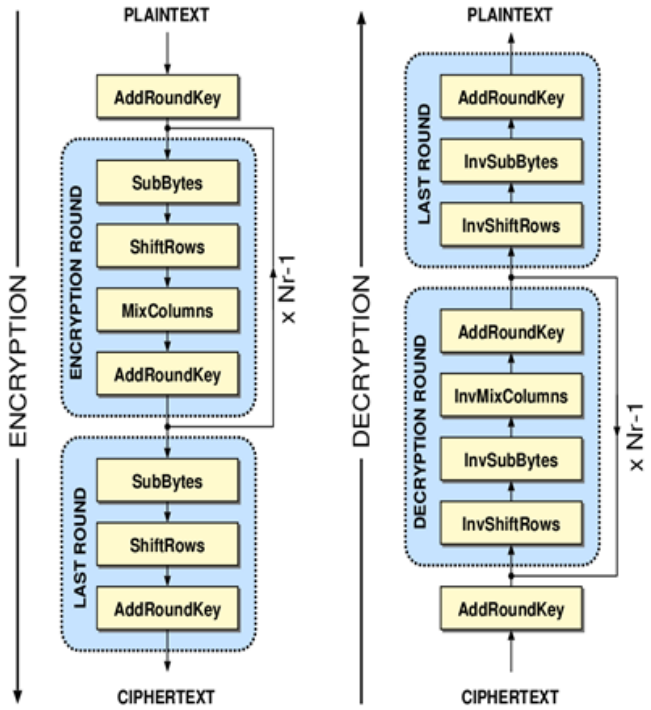

Fig.2. The principle of operation of the AES encryption algorithm [4]

As a symmetric algorithm, AES uses the same key for both encryption and decryption of data. It is extensively used in various fields, including secure communication protocols, disk and file encryption. AES has proven to be an extremely reliable algorithm, providing protection against many types of attacks, especially when using a 256-bit key.

The difference in security levels between 128-bit and 256-bit AES keys is significant. While AES-128 is already considered highly secure and is widely used, AES-256 offers an even higher level of protection. A 128-bit key has 2^128 possible combinations, whereas a 256-bit key has 2^256 combinations. This means that a brute-force attack on a 256-bit key would require significantly more time and computational resources compared to an attack on a 128-bit key.

Attempting to crack a 128-bit AES key by brute force requires enormous computational power and time, even for supercomputers. The exact time to crack depends on various factors such as processor speed, parallelization efficiency, and the attack algorithm used. Rough estimates suggest that a brute-force attack on a 128-bit key would take several billion years, which is beyond the capabilities of current and foreseeable computing technology.

http://dx.doi.org/10.31364/SCIRJ/v12.i08.2024.P0824992

It is important to note that brute-force attacks are not the only way to break a cryptographic system. Other types of attacks, such as side-channel attacks, exploit vulnerabilities in cryptographic systems as physical objects. Therefore, it is essential to adhere to cryptographic best practices and stay updated with current security recommendations and updates for the chosen algorithm.

RSA (Rivest-Shamir-Adleman), on the other hand, is a widely used asymmetric encryption algorithm based on the difficulty of factoring large prime numbers. When using sufficiently long keys, such as 2048 bits or more, RSA is considered secure for many applications.

An example of RSA usage is the SSH (Secure Shell) protocol, which provides secure connections between systems. RSA is used for key-based authentication in SSH. A user generates a pair of keys, with the private key stored on the local system and the public key uploaded to the remote system to encrypt challenge messages, which are then decrypted using the private key. Successful decryption authenticates the user.

It is worth noting that SSH supports various encryption algorithms and key types, including DSA and ECDSA, as well as symmetric algorithms such as AES, Blowfish, and 3DES. The specific encryption algorithm depends on the SSH client and server configuration.

When comparing these algorithms, RSA and AES represent two fundamentally different types of encryption designed for different purposes. RSA, being an asymmetric algorithm, uses two keys—public and private—and is used for tasks such as key exchange, digital signatures, and secure communication channels. AES, in contrast, is a symmetric algorithm using the same key for encryption and decryption. It is widely used for encrypting data when both the sender and receiver have the same key.

Both algorithms are considered reliable when used correctly. However, their security depends on key length and implementation specifics. Generally, longer keys provide higher security. RSA and AES support key lengths considered highly secure. AES, however, is more efficient and faster for encrypting large volumes of data. A comparison of these encryption algorithms is provided in Table 2 [5].

Table 2. Comparison of AES and RSA encryption methods

Attribute	**AES**	**RSA**
Type	Symmetric key encryption	Asymmetric encryption (public key)
Key Length	128, 192, or 256 bits	1024, 2048, or 4096 bits (common)
Speed and Efficiency	Fast and efficient for large data volumes	Slower, not suitable for large data volumes
Use Cases	File encryption, databases, and channels	Key exchange, authentication, signatures
Encryption Process	Substitution-permutation network	Modular exponentiation
Key Distribution	Requires a secure method to transfer the secret key	No need to securely transfer the public key
Computational Complexity	Relatively low	High, especially for longer keys

http://dx.doi.org/10.31364/SCIRJ/v12.i08.2024.P0824992

Resistance to Attacks	Vulnerable to brute force attacks but still secure	Vulnerable to advances in factoring methods
Key Management	Simpler, as only one key is involved	More complex due to separate public and private keys
Hardware Suitability	Well-suited for hardware implementation	Hardware implementation can be more complex
Quantum Resistance	Vulnerable to quantum attacks (e.g., Grover's algorithm)	Potentially vulnerable to quantum attacks
Example	Secure file storage and data exchange	Secure email and digital certificates

Therefore, through the application of cloud encryption, it is possible to ensure:

- Data Security: Cloud encryption is a powerful tool for preventing data breaches and cyberattacks. Whether the data resides in cloud storage or is being transmitted between users, encryption ensures its protection.
- Facilitation of Collaboration: Cloud encryption allows enterprises to securely utilize cloud services for collaborative work. Authorized users can exchange encrypted data without fear of leaks or cyberattacks.
- Guarantee of Authenticity and Integrity: End-to-end encryption prevents unauthorized modifications of data, ensuring its authenticity and integrity both during storage and transmission.
- Compliance with Regulatory Requirements: Cloud encryption helps enterprises meet various legislative and regulatory data protection requirements, such as HIPAA, FIPS, and PCI DSS.

However, there are also challenges primarily related to the following factors:

- Performance and Integration Difficulties: Previously, performance and integration issues often hindered the adoption of encryption. Encryption was considered complex and inconvenient for users who needed frequent access to files from various devices. Modern systems have become faster and more user-friendly, but it is important to conduct trial testing of the platform to ensure it meets integration and usability requirements.
- Resource Consumption: The encryption process requires significant resources, leading to additional time and cost expenditures for daily operations. It is important to monitor access times and resource usage levels for effective management.
- Risk of Encryption Key Loss: Losing encryption keys can render data inaccessible. Inadequate key management can jeopardize critical data, so it is necessary to ensure secure storage and management of keys.
- Configuration: A key issue is the proper setup of cloud encryption services. Security strategy gaps can occur if administrators assume data is encrypted when, in fact, configuration errors leave it vulnerable [7].

Conclusion

The AES and RSA algorithms examined in this work demonstrate high efficiency in protecting data stored in cloud services. The use of symmetric encryption, represented by the AES algorithm, allows for high data processing speeds, which is critically

http://dx.doi.org/10.31364/SCIRJ/v12.i08.2024.P0824992

important for large cloud storage systems with significant volumes of information. The RSA asymmetric algorithm, in turn, provides reliable encryption key protection, substantially enhancing overall system security. The combined use of these methods creates an optimal balance between speed and security. Thus, the correct selection and application of encryption algorithms are key factors for data protection in cloud storage, especially amid growing cyber threats. Further research in this area may focus on optimizing existing methods and developing new approaches to more effectively ensure data security in cloud environments.

References

1. Cloud Storage Security and Data Encryption. [Electronic resource] Access mode: https://www.unspiring.com/post/cloud-storage-security-and-data-encryption (access date 06/25/2024).
2. How to Encrypt Cloud Storage in 2024: Secure Your Stored Files With Encryption. [Electronic resource] Access mode: https://www.cloudwards.net/how-to-encrypt-your-data-for-cloud-storage/ (access date 06/25/2024).
3. Encryption: Understanding the Role of Encryption in Cloud Storage. [Electronic resource] Access mode: https://fastercapital.com/content/Encryption--Understanding-the-Role-of-Encryption-in-Cloud-Storage.html (access date 06/25/2024).
4. A Comparative Analysis on AES and RSA Algorithms. [Electronic resource] Access mode: https://www.researchgate.net/publication/292150298_A_Comparative_Analysis_on_AES_and_RSA_Algorithms/link/56ab298d08ae8f38656751b4/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19 (accessed 06/25/2024).
5. Cryptographic Algorithms: A Comparison of Security and Strength. [Electronic resource] Access mode: https://www.kapresoft.com/software/2023/05/07/cryptography-algorithms-comparison.html (access date 06/25/2024).
6. Difference Between AES and RSA Encryption. [Electronic resource] Access mode: https://www.geeksforgeeks.org/difference-between-aes-and-rsa-encryption/ (access date 06/25/2024).
7. Cloud encryption. [Electronic resource] Access mode: https://www.techtarget.com/searchstorage/definition/cloud-encryption-cloud-storage-encryption (access date 06/25/2024).

http://dx.doi.org/10.31364/SCIRJ/v12.i08.2024.P0824992