WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Secure File Storage Using Hybrid Cryptography on Cloud

Ritik Tyagi[1], Ritika Tyagi[2], Riya Verma[3]

Raj Kumar Goel Institute of Technology Ghaziabad, India

ABSTRACT :

Secure file storage using hybrid cryptography on the cloud is an innovative approach designed to enhance data security by combining the strengths of both symmetric and asymmetric cryptographic techniques.

This hybrid cryptography system leverages the speed and efficiency of symmetric encryption algorithms, such as AES (Advanced Encryption Standard), to encrypt the data files. These algorithms are known for their high performance and low computational overhead, making them suitable for encrypting large volumes of data. However, the management and distribution of symmetric keys pose a significant security risk.

To address this, asymmetric cryptographic algorithms, like RSA (Rivest-Shamir-Adleman), are employed to securely exchange the symmetric keys. Asymmetric encryption, while computationally more intensive, provides a robust mechanism for key distribution, ensuring that the symmetric keys are securely transmitted between the data owner and the cloud storage provider.

The proposed system architecture involves a multi-layered security framework. Initially, the data is encrypted using a symmetric key. This symmetric key is then encrypted with the recipient's public key using asymmetric encryption. The encrypted data and the encrypted symmetric key are stored in the cloud. During retrieval, the recipient uses their private key to decrypt the symmetric key, which is then used to decrypt the data files.

This dual-layer encryption model not only secures the data during storage and transmission but also provides a fail-safe mechanism against potential breaches. Even if the encrypted data is intercepted, without the corresponding private key, it remains inaccessible, ensuring confidentiality and integrity.

The implementation of hybrid cryptography in cloud storage addresses critical security issues, including unauthorized access, data breaches, and key management challenges. By combining the advantages of both cryptographic methods, it offers a robust and efficient solution for secure cloud-based file storage, making it a viable option for enterprises looking to safeguard their sensitive information in the cloud.

Keywords - Hybrid Cryptography, Cloud Storage, Symmetric Encryption, Asymmetric Encryption, Data Security, Key Management, AES, RSA.

Introduction:

In today's digital era, cloud computing has emerged as a pivotal technology, enabling convenient, on-demand access to a shared pool of configurable computing resources. This paradigm shift has brought about significant changes in data storage, allowing individuals and organizations to store vast amounts of data remotely, thus eliminating the need for local storage infrastructure and reducing associated costs. However, with these benefits come substantial security challenges, particularly regarding the protection of sensitive information stored in the cloud.

As cloud services become increasingly integral to business operations, ensuring the confidentiality, integrity, and availability of data has become paramount. Traditional encryption techniques have been employed to safeguard data, but each method comes with its own set of limitations. Symmetric encryption algorithms, such as the Advanced Encryption Standard (AES), are known for their efficiency and speed, making them suitable for encrypting large datasets. However, the primary drawback of symmetric encryption lies in key distribution and management, as securely sharing and storing keys can be problematic.

On the other hand, asymmetric encryption algorithms, such as the Rivest-Shamir-Adleman (RSA) algorithm, offer a solution to the key distribution problem by using a pair of cryptographic keys – a public key for encryption and a private key for decryption. Despite their security advantages, asymmetric algorithms are computationally intensive and less efficient for encrypting large volumes of data.

To leverage the strengths and mitigate the weaknesses of both cryptographic methods, a hybrid cryptography approach is proposed for secure file storage on the cloud. Hybrid cryptography combines the speed and efficiency of symmetric encryption with the secure key distribution capabilities of asymmetric encryption, offering a comprehensive solution for data security.

In this hybrid model, data files are encrypted using a symmetric algorithm, such as AES, ensuring quick and efficient encryption and decryption processes. The symmetric key used for this encryption is then secured using an asymmetric algorithm, such as RSA, which encrypts the symmetric key with the recipient’s public key. This encrypted symmetric key is then stored alongside the encrypted data in the cloud.

During the data retrieval process, the recipient uses their private key to decrypt the symmetric key. The decrypted symmetric key is then used to decrypt the data files, ensuring that only authorized users can access the stored information. This dual-layer encryption strategy not only secures data against unauthorized access but also provides a robust mechanism for key management.
By integrating hybrid cryptography into cloud storage solutions, it is possible to achieve a higher level of security, addressing common concerns such as unauthorized data access, breaches, and efficient key management

Literature Review

The rapid adoption of cloud computing has transformed data storage practices, prompting extensive research into secure storage methods to protect sensitive information. This literature review explores the evolution and current state of secure file storage using hybrid cryptography in the cloud, focusing on the advantages, challenges, and implementation strategies of this approach.

Cloud Storage Security Concerns

Several studies have highlighted the primary security concerns associated with cloud storage, including unauthorized access, data breaches, and data integrity issues. According to Subashini and Kavitha (2011), cloud environments are susceptible to various threats due to their multi-tenant nature and shared resources. These vulnerabilities necessitate robust security mechanisms to ensure data protection.

Symmetric Encryption

Symmetric encryption, particularly the Advanced Encryption Standard (AES), is widely recognized for its efficiency in encrypting large datasets. In a study by Daemen and Rijmen (2002), AES was demonstrated to be highly secure and computationally efficient, making it suitable for cloud storage applications. However, managing and securely distributing symmetric keys remains a significant challenge, as highlighted by Gupta and Gupta (2016).

Asymmetric Encryption

Asymmetric encryption techniques, such as RSA, provide a solution to the key distribution problem inherent in symmetric encryption. Rivest, Shamir, and Adleman (1978) introduced RSA, emphasizing its ability to use public and private key pairs for secure key exchange. Despite its security advantages, RSA is computationally intensive, making it less practical for encrypting large volumes of data.

Hybrid Cryptography

To address the limitations of both symmetric and asymmetric encryption, hybrid cryptographic systems have been proposed. In a hybrid system, symmetric encryption is used to encrypt the data, and asymmetric encryption is used to securely transmit the symmetric key. This approach leverages the strengths of both encryption methods while mitigating their weaknesses.

Implementations of Hybrid Cryptography in Cloud Storage

Recent research has explored various implementations of hybrid cryptography in cloud storage. For instance, a study by Alzain, Soh, and Pardede (2013) proposed a hybrid encryption framework that combines AES and RSA to secure cloud data. Their framework encrypts the data with AES and the AES key with RSA, ensuring efficient encryption and secure key management.
Similarly, Kaur and Kinger (2014) developed a hybrid cryptographic model utilizing AES and RSA for secure cloud storage. Their model demonstrated improved security and performance compared to using either encryption method alone.

Algorithms Used

In secure file storage using hybrid cryptography on the cloud, a combination of symmetric and asymmetric encryption algorithms is employed to leverage the strengths of both types of cryptography. Here are the primary algorithms typically used:

Symmetric Encryption Algorithms

1. *Advanced Encryption Standard (AES)*
    - *Description*: AES is a widely-used symmetric encryption algorithm known for its high performance and strong security. It encrypts data in fixed block sizes (128 bits) using key sizes of 128, 192, or 256 bits.
    - *Application*: AES is often used to encrypt the actual data files in cloud storage due to its efficiency in handling large volumes of data quickly.
2. *Blowfish*
    - *Description*: Blowfish is another symmetric block cipher known for its speed and effectiveness. It works with variable key lengths from 32 to 448 bits, providing flexibility in encryption strength.
    - *Application*: While less common than AES, Blowfish can be used for data encryption in hybrid systems, especially when a faster algorithm with variable key lengths is needed.

Asymmetric Encryption Algorithms

1. *Rivest-Shamir-Adleman (RSA)*
    - *Description*: RSA is a widely-used asymmetric encryption algorithm that uses a pair of keys (public and private) for encryption and decryption. It relies on the computational difficulty of factoring large integers.
    - *Application*: In hybrid cryptographic systems, RSA is typically used to encrypt the symmetric key that encrypts the data. This ensures secure key exchange between parties.
2. *Elliptic Curve Cryptography (ECC)*
    - *Description*: ECC provides similar security to RSA but with smaller key sizes, making it more efficient in terms of computational overhead and resource usage. ECC is based on the algebraic structure of elliptic curves over finite fields.
    - *Application*: ECC can be used to encrypt the symmetric key in a hybrid system, offering enhanced security and performance benefits compared to RSA.

Hash Functions

1. *SHA-256 (Secure Hash Algorithm 256-bit)*
    - *Description*: SHA-256 is part of the SHA-2 family and produces a 256-bit hash value. It is widely used for ensuring data integrity.
    - *Application*: SHA-256 can be used to verify the integrity of the data stored and transmitted, ensuring that the data has not been altered.
2. *MD5 (Message Digest Algorithm 5)*
    - *Description*: MD5 produces a 128-bit hash value, but it is less secure than SHA-256 due to vulnerabilities to collision attacks.
    - *Application*: While generally avoided in modern systems due to its vulnerabilities, MD5 might still be found in legacy systems for hash functions.

Hybrid Encryption Workflow

1. *Data Encryption*:
    - The data file is encrypted using a symmetric algorithm (e.g., AES). This ensures that the encryption process is fast and suitable for large data volumes.
2. *Key Encryption*:
    - The symmetric key used to encrypt the data is then encrypted using an asymmetric algorithm (e.g., RSA or ECC). This step secures the symmetric key, facilitating safe transmission and storage.
3. *Storage*:
    - Both the encrypted data and the encrypted symmetric key are stored in the cloud. The separation of data encryption and key encryption ensures that unauthorized access to the data requires compromising both the symmetric key and the encrypted key.
4. *Data Retrieval*:
    - The recipient first decrypts the symmetric key using their private key (asymmetric decryption).
    - The decrypted symmetric key is then used to decrypt the data file (symmetric decryption).

Proposed Model

The proposed model for secure file storage using hybrid cryptography on the cloud integrates symmetric and asymmetric encryption techniques to ensure robust data security and efficient key management. The model is designed to address the security concerns of unauthorized access, data breaches, and efficient key distribution while maintaining performance and scalability. Below is a detailed description of the proposed model, including its components and workflow.

Components

1. *Client Device*: The device used by the end-user to upload, store, and retrieve files from the cloud.
2. *Cloud Storage Provider*: The cloud service that provides storage infrastructure and services.
3. *Encryption Module*: Software or hardware module on the client device that handles encryption and decryption processes.
4. *Key Management Server (KMS)*: A dedicated server responsible for generating, storing, distributing, and managing encryption keys.

Workflow

1. *File Upload and Encryption*
    - *Step 1: File Selection*: The user selects the file to be uploaded to the cloud storage.
    - *Step 2: Symmetric Encryption*: The file is encrypted using a symmetric encryption algorithm (e.g., AES-256). This step ensures that the file is securely encrypted before leaving the client device.
        - Generate a symmetric key (SK).
        - Encrypt the file using SK and AES-256.
    - *Step 3: Asymmetric Encryption of Symmetric Key*: The symmetric key (SK) is then encrypted using the recipient's public key with an asymmetric encryption algorithm (e.g., RSA-2048 or ECC).
        - Retrieve the recipient's public key (PK).

        - Encrypt SK using PK to produce an encrypted symmetric key (ESK).
    - *Step 4: Data Packaging*: The encrypted file and the encrypted symmetric key (ESK) are packaged together for storage.
        - Create a package containing the AES-encrypted file and the RSA/ECC-encrypted symmetric key.
2. *File Storage*
    - *Step 5: Upload to Cloud*: The package containing the encrypted file and the encrypted symmetric key is uploaded to the cloud storage provider.
        - Transmit the encrypted package to the cloud.
    - *Step 6: Storage*: The cloud storage provider stores the encrypted package securely in the cloud infrastructure.
        - Store the package in the cloud storage database.
3. *File Retrieval and Decryption*
    - *Step 7: Download from Cloud*: The user requests to download the encrypted file from the cloud storage.
        - Retrieve the encrypted package from the cloud.
    - *Step 8: Decryption of Symmetric Key*: The encrypted symmetric key (ESK) is decrypted using the user's private key (SK).
        - Retrieve the user's private key.
        - Decrypt ESK using the private key to obtain the original symmetric key (SK).
    - *Step 9: Symmetric Decryption*: The encrypted file is decrypted using the symmetric key (SK) to restore the original file.
        - Use SK to decrypt the AES-encrypted file.
4. *Key Management*
    - *Step 10: Key Management Operations*: The KMS handles the lifecycle of keys, including generation, distribution, rotation, and revocation.
        - Generate and distribute asymmetric key pairs (public and private keys).
        - Store and manage symmetric keys securely.
        - Rotate and revoke keys as needed based on security policies.

Conclusion

The literature indicates that hybrid cryptography is a promising solution for secure file storage in the cloud, offering a balanced approach to data encryption and key management. While there are challenges to be addressed, ongoing research and technological advancements are likely to enhance the viability and effectiveness of hybrid cryptographic systems in cloud environments. Future studies should focus on optimizing these systems for performance, scalability, and ease of integration to fully realize their potential in securing cloud storage.

Future Scope

As cloud computing continues to evolve, the demand for secure file storage solutions will intensify, driven by increasing data volumes, stringent regulatory requirements, and sophisticated cyber threats. Hybrid cryptography, which combines the strengths of symmetric and asymmetric encryption, offers a promising path forward for enhancing data security in the cloud. The future scope of secure file storage using hybrid cryptography includes several key areas of development and research:

1. Enhanced Key Management Systems

Future advancements will focus on developing more sophisticated key management systems that can handle the complexities of hybrid cryptographic frameworks. This includes automated key generation, distribution, rotation, and revocation processes, ensuring seamless and secure management of both symmetric and asymmetric keys. Integrating advanced technologies like blockchain for decentralized key management could also provide robust solutions to prevent unauthorized access and ensure data integrity.

2. Performance Optimization

As data volumes continue to grow, optimizing the performance of hybrid cryptographic systems will become critical. Future research will aim to reduce the computational overhead associated with encryption and decryption processes, potentially through hardware acceleration, parallel processing, and more efficient algorithms. Machine learning techniques might also be applied to predict and optimize encryption workflows, further enhancing system performance.

3. Scalability and Integration

Hybrid cryptography solutions will need to scale seamlessly with growing cloud infrastructure and integrate effortlessly with existing cloud services. Developing scalable architectures that can handle large-scale deployments while maintaining high levels of security will be essential. Additionally, ensuring compatibility with various cloud service providers and platforms will facilitate wider adoption and interoperability.

REFERENCES:

1. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1), 1-11.

2. Daemen, J., & Rijmen, V. (2002). The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media.
3. Gupta, M., & Gupta, S. (2016). Symmetric key cryptography: Current trends. *International Journal of Computer Applications*, 150(12), 8-11.
4. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120-126.
5. Alzain, M. A., Soh, B., & Pardede, E. (2013). A survey on data security issues in cloud computing: From single to multi-clouds. *Journal of Software*, 8(5), 1068-1078.
6. Kaur, A., & Kinger, S. (2014). A survey of hybrid encryption techniques. *International Journal of Computer Applications*, 103(12).
7. Singh, S., & Supriya. (2013). A review of cryptographic algorithms. *International Journal of Security and Its Applications*, 7(4), 97-106.