iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** XI **Month of publication:** November 2024

DOI: https://doi.org/10.22214/ijraset.2024.65674

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue XI Nov 2024- Available at www.ijraset.com

Secured Data Storage on the Cloud Using Hybrid Cryptography

Manas Bhawane[1], Prof. Simran Ahuja[2]
Member, Keystone School of Engineering

Abstract: ***With the growing reliance on cloud computing for data storage, ensuring the security and confidentiality of sensitive data has become paramount. Despite its advantages, cloud storage is susceptible to various security threats such as data breaches, unauthorized access, and insider threats. Traditional cryptographic techniques like symmetric and asymmetric cryptography offer a measure of security but have limitations when used independently. This paper proposes a hybrid cryptographic approach that combines the strengths of both symmetric and asymmetric cryptography, ensuring a robust solution for secured data storage in the cloud. The hybrid approach leverages the speed and efficiency of symmetric algorithms and the strong security features of asymmetric algorithms, making them both secure and efficient. This research explores various hybrid encryption techniques, discusses their security features, and demonstrates how they enhance data protection on cloud platforms.***
Keywords: Cloud Storage, Hybrid Cryptography, Symmetric Encryption, Asymmetric Encryption, Data Security

I. INTRODUCTION

With the increasing adoption of cloud computing, businesses and individuals are moving their data to cloud-based platforms for scalability, accessibility, and cost efficiency. However, as more data is stored on cloud servers, the need for robust security mechanisms has become crucial. Cloud storage presents multiple security challenges, including data confidentiality, data integrity, and the protection of data from unauthorized access. Various cryptographic techniques are employed to address these concerns.

The primary objective of this research is to propose a hybrid cryptographic model that integrates both symmetric and asymmetric encryption techniques to provide enhanced security for data stored in the cloud. Symmetric encryption offers fast and efficient encryption, but key management is a significant challenge. On the other hand, asymmetric encryption provides more secure key distribution but is computationally expensive. The combination of these two techniques in a hybrid cryptography model offers both efficiency and enhanced security.

II. CLOUD STORAGE SECURITY CHALLENGES

The main security issues associated with cloud storage include:

1) *Data Confidentiality:* Data stored in the cloud must remain confidential and protected from unauthorized access. Data confidentiality ensures that only authorized users can view or manipulate sensitive information.
2) *Data Integrity:* Ensuring that data remains unchanged and unaltered during storage or transmission is critical. Data integrity is often compromised during cyberattacks or hardware failures.
3) *Authentication and Authorization:* Verifying the identity of users accessing the cloud storage system is essential to prevent unauthorized access to sensitive data.
4) *Data Availability:* Cloud service providers must ensure continuous availability of data for authorized users without compromising security.

Traditional security methods address these issues to some extent, but as the sophistication of attacks increases, these methods may not be sufficient.

III. CRYPTOGRAPHIC TECHNIQUES FOR DATA SECURITY

Cryptography is widely used to secure data in the cloud. There are two main types of cryptographic techniques:

A. Symmetric Encryption

In symmetric encryption, the same key is used for both encryption and decryption. Algorithms like AES (Advanced Encryption Standard) and DES (Data Encryption Standard) fall under this category. Symmetric encryption is fast and efficient but suffers from the key distribution problem — securely sharing the key between parties is challenging.

B. Asymmetric Encryption

Asymmetric encryption uses a pair of keys: a public key for encryption and a private key for decryption. RSA (Rivest–Shamir–Adleman) and ECC (Elliptic Curve Cryptography) are examples of asymmetric algorithms. While key distribution is more secure, asymmetric encryption is slower than symmetric encryption due to the complexity of the mathematical operations involved.

IV. PROPOSED HYBRID CRYPTOGRAPHIC MODEL

To address the limitations of both symmetric and asymmetric encryption, this research proposes a hybrid cryptographic model that combines the two. The proposed system follows these steps:

A. Encryption Process

1) Step 1: Symmetric Encryption: The plaintext data is first encrypted using a fast symmetric algorithm like AES. A secret symmetric key is generated for this process.
2) Step 2: Asymmetric Key Encryption: The symmetric key used in Step 1 is then encrypted using the recipient's public key (asymmetric encryption using RSA or ECC).
3) Step 3: Data Storage: The encrypted data (ciphertext) and the encrypted symmetric key are both stored on the cloud server.

B. Decryption Process

1) Step 1: Asymmetric Decryption: When the user wishes to retrieve the data, the encrypted symmetric key is decrypted using the user's private key.
2) Step 2: Symmetric Decryption: The decrypted symmetric key is then used to decrypt the stored ciphertext, restoring the original plaintext data.

By combining symmetric and asymmetric encryption, the system takes advantage of the fast processing of symmetric algorithms while securing key distribution with asymmetric encryption.

V. ADVANTAGES

The proposed hybrid cryptographic model offers several advantages over traditional cryptography:

1) *Enhanced Security:* The combination of two encryption methods adds a layer of security. Even if the cloud service provider or an attacker gains access to the encrypted data, they cannot decrypt it without both the private key and the symmetric key.
2) *Efficient Key Management:* By using asymmetric encryption for key distribution, the issues of key management and secure transmission in symmetric encryption are resolved.
3) *Improved Performance:* The computationally expensive asymmetric encryption is applied only to the symmetric key, not the entire dataset. This results in faster encryption and decryption processes compared to using asymmetric encryption alone.

VI. DISADVANTAGES

1) *Complexity:* Implementing both symmetric and asymmetric encryption adds complexity to system design, increasing the risk of errors and higher development costs.
2) *Performance Overhead:* The use of asymmetric encryption for key management introduces computational overhead, leading to slower data access compared to purely symmetric encryption.
3) *Key Management Challenges:* Proper handling of encryption keys, especially private keys, remains a challenge, and key compromise can lead to system vulnerabilities.
4) *Secure Key Storage Dependence:* The security of the system heavily depends on the secure storage of private keys. If compromised, the data encryption is rendered ineffective.
5) *Scalability Issues:* As data size or user count increases, key management and encryption can become resource-intensive, affecting system performance.
6) *Vulnerability to Attacks:* Hybrid cryptography can still be susceptible to brute-force, man-in-the-middle, or key exposure attacks.
7) *Resource Consumption:* Asymmetric encryption requires significant computational resources, which can lead to higher costs and slower processing in cloud environments.
8) *Key Revocation Complexity:* Revoking and replacing compromised keys is a slow and resource-heavy process, especially in large systems.

9) *Cloud Provider Dependence:* The overall security of the system also depends on the security infrastructure of the cloud service provider, which may introduce additional risks.

VII. APPLICATION

Hybrid cryptography can be used in various cloud storage applications:

1) *Enterprise Cloud Storage:* Large enterprises store sensitive customer data in the cloud. The hybrid approach ensures both the confidentiality and integrity of this data.
2) *Healthcare Systems:* Patient health records stored in the cloud require strong encryption methods to protect privacy. The proposed system can ensure secure data storage while allowing authorized personnel to access the information.
3) *Financial Data:* Financial institutions rely on secure cloud storage to protect customer transaction data. The hybrid cryptography model prevents unauthorized access and ensures secure key management.

VIII. SECURITY ANALYSIS

To evaluate the security of the proposed hybrid cryptographic model, several key security properties are considered:

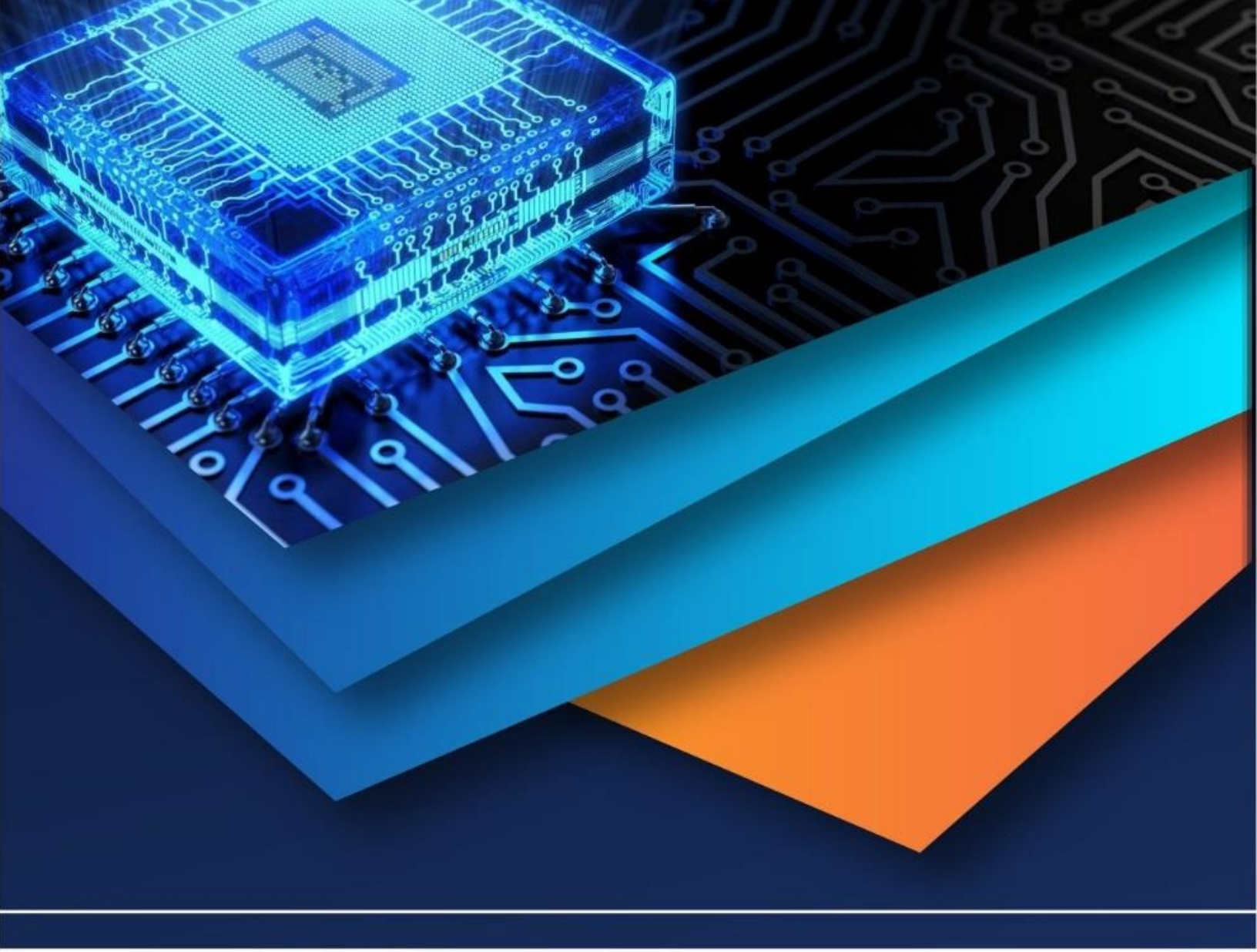
1) *Confidentiality:* The combination of symmetric and asymmetric encryption ensures that the data remains confidential, even in the case of a data breach.
2) *Integrity:* By adding cryptographic checks such as hashing and digital signatures, the integrity of the data can be guaranteed.
3) *Authentication:* Asymmetric encryption allows for the implementation of public key infrastructure (PKI), which enhances authentication and ensures that only authorized users can decrypt the data.

IX. CONCLUSION

As cloud storage becomes more ubiquitous, securing sensitive data stored on the cloud is essential. This paper proposes a hybrid cryptographic approach that leverages the strengths of both symmetric and asymmetric encryption to ensure enhanced data security. By using fast symmetric encryption for the data and secure asymmetric encryption for key management, the proposed model ensures that data stored in the cloud is secure and efficient. The hybrid cryptography model offers a practical solution for addressing key management challenges and ensuring data confidentiality, integrity, and availability in cloud environments.

REFERENCES

[1] Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson.
[2] Menezes, A., van Oorschot, P., & Vanstone, S. (1996). Handbook of Applied Cryptography. CRC Press.
[3] 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.
[4] Diffie, W., & Hellman, M. E. (1976). "New Directions in Cryptography." IEEE Transactions on Information Theory, 22(6), 644-654.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY