Short Communication

IMedPub Journals
www.imedpub.com

American Journal of Computer Science and Information Technology
ISSN 2349-3917

2025
Vol.13 No.1:5

Hybrid Encryption Algorithms for Cloud Data Protection

Carlos Fernandez*

Department of Software Engineering, National Autonomous University of Mexico (UNAM), Mexico City 04510, Mexico

***Corresponding author:** Carlos Fernandez, Department of Software Engineering, National Autonomous University of Mexico (UNAM), Mexico City 04510, Mexico; E-mail: fernandezcarlos01@unam.mx

Received date: January 01, 2025, Manuscript No. Ipacsit-25-20922; **Editor assigned date:** January 03, 2025, PreQC No. ipacsit-25-20922 (PQ); **Reviewed date:** January 20, 2025, QC No. ipacsit-25-20922; **Revised date:** January 27, 2025, Manuscript No. ipacsit-25-20922 (R); **Published date:** February 4, 2025, DOI: 10.36648/2349-3917.13.1.5

Citation: Fernandez C (2025) Hybrid Encryption Algorithms for Cloud Data Protection. Am J Compt Sci Inform Technol Vol.13 No.1:5

Introduction

In the era of digital transformation, cloud computing has emerged as the backbone of modern data management, offering scalable storage, flexible resource allocation, and global accessibility. However, as vast amounts of sensitive information including personal, financial, and organizational data are stored and processed in the cloud, data security has become a critical concern. Traditional encryption techniques, while effective, often struggle to balance the trade-offs between performance and security in such dynamic environments. To address this, hybrid encryption algorithms have gained prominence as a robust solution for ensuring cloud data protection. These algorithms combine the strengths of both symmetric and asymmetric encryption methods, achieving a balance between computational efficiency and secure key management. By leveraging the speed of symmetric encryption for data transmission and the security of asymmetric encryption for key exchange, hybrid encryption provides a comprehensive framework that safeguards data integrity, confidentiality, and availability in cloud computing environments [1].

Description

Hybrid encryption algorithms function through a two-tiered approach that integrates symmetric and asymmetric cryptographic techniques. In this model, symmetric algorithms such as Advanced Encryption Standard (AES) or Data Encryption Standard (DES) are used to encrypt large volumes of data efficiently, as they require less computational power and provide faster encryption and decryption processes. However, the major challenge with symmetric encryption lies in secure key distribution if the secret key is intercepted, the entire system is compromised. To mitigate this, hybrid encryption uses asymmetric algorithms like RSA or Elliptic Curve Cryptography (ECC) to encrypt the symmetric key itself before transmission. The recipient can then decrypt the symmetric key using their private key, ensuring that only authorized users can access the encrypted data [2].

Furthermore, hybrid encryption can be integrated with digital signatures to ensure data authenticity, allowing users to verify that the received information has not been altered during transmission. Another critical advantage of hybrid encryption lies in its adaptability to various cloud architectures, including public, private, and hybrid clouds. Cloud service providers often handle data from multiple users, making key management and data isolation vital. Hybrid encryption addresses this by using hierarchical key management systems, where unique encryption keys are generated for each user or dataset, reducing the risk of cross-data compromise [3].

Additionally, the combination of symmetric and asymmetric encryption allows for scalable protection mechanisms that can secure both data-at-rest and data-in-transit. For example, stored files can be encrypted using symmetric methods for efficiency, while transmission between users and cloud servers can utilize asymmetric encryption for secure communication. Researchers have also explored the integration of hybrid encryption with emerging technologies such as block chain and homomorphic encryption to strengthen data integrity and enable secure computations over encrypted data. Despite challenges such as computational overhead and complex implementation, hybrid encryption continues to evolve as a reliable solution that balances performance, scalability, and high-level security in cloud ecosystems [4,5].

Conclusion

In conclusion, hybrid encryption algorithms represent a significant advancement in cloud data protection by combining the efficiency of symmetric encryption with the robust key management of asymmetric methods. This dual-layered approach ensures that cloud-stored and transmitted data remain secure against unauthorized access, interception, and tampering. The adaptability of hybrid encryption makes it an ideal solution for modern cloud infrastructures, addressing both performance and security concerns. As cloud computing continues to expand across industries, the implementation of hybrid encryption will play an essential role in building user trust, ensuring compliance with data protection regulations, and safeguarding critical digital assets. Future developments, including the integration of quantum-resistant cryptographic techniques, will further strengthen hybrid encryption's role as the cornerstone of secure, efficient, and resilient cloud computing environments.

Acknowledgement

None

Conflict of Interest

None

References

1. Jin X, Duan X, Jin H, Ma Y (2020) A novel hybrid secure image encryption based on the shuffle algorithm and the hidden attractor chaos system. Entropy 22: 640

2. ElKamchouchi DH, Mohamed HG, Moussa KH (2020) A bijective image encryption system based on hybrid chaotic map diffusion and DNA confusion. Entropy 22: 180

1. Ravichandran D, Praveenkumar P, Rayappan JBB, Amirtharajan R (2016) Chaos based crossover and mutation for securing DICOM image. Comput Biol Med 72: 170–184

3. Li C, Zhang J, Sang L, Gong L, Wang L, et al. (2020) Deep learning-based security verification for a random number generator using white chaos. Entropy 22: 1134

4. Singh P, Devi KJ, Thakkar HK, Santamaria J (2021) Blind and secured adaptive digital image watermarking approach for high imperceptibility and robustness. Entropy 23: 1650