HYBRID CLOUD SECURITY: REVERSE DATA HIDING TECHNIQUES FOR ENCRYPTED STORAGE

N. Subalakshmi[*1], M. Jeyakarthic[2]
[*1]Assistant Professor,Computer Science and Engineering Wing, Directorate of Distance Education, Annamalai University, Annamalai Nagar, Tamil Nadu, India. subhaabi12@gmail.com
[2]Assistant Professor, Department of Computer and Information Science, Annamalai University, Chidambaram, Tamilnadu, India.jeya_karthic@yahoo.com

ABSTRACT
The increasing adoption of hybrid cloud environments presents new challenges for ensuring the security and privacy of sensitive data. This paper introduces the Encrypted Storage with Dynamic Reverse Hiding (ESDRH) algorithm, a novel approach designed to enhance hybrid cloud security through advanced reverse data hiding techniques for encrypted storage. The ESDRH algorithm encompasses four key components: Dynamic Key Generation (DKG), Adaptive Encryption (AE), Reverse Data Embedding (RDE), and Integrity Verification and Access Control (IVAC).Dynamic Key Generation (DKG) creates unique encryption keys for each data session, reducing the risk of key compromise. Adaptive Encryption (AE) combines symmetric and asymmetric encryption methods to optimize security and performance. Reverse Data Embedding (RDE) embeds unique identifiers and metadata within encrypted data blocks, ensuring data integrity and facilitating efficient management without compromising privacy. This technique allows for the secure distribution of encrypted data blocks across public and private cloud resources, enhancing both security and access efficiency. Integrity Verification and Access Control (IVAC) mechanisms are implemented to ensure that only authorized users can access the stored data, employing multi-factor authentication and continuous monitoring. Upon retrieval, data blocks are verified for integrity and decrypted, ensuring that the original content remains intact and accessible solely by legitimate users. The ESDRH algorithm offers a scalable, user-friendly solution to the complexities of data security in hybrid cloud environments, leveraging innovative reverse data hiding techniques to significantly improve data protection, compliance, and operational efficiency. This approach represents a substantial advancement in the secure management of encrypted storage in modern cloud infrastructures.

Keywords: Hybrid Cloud Security, Reverse Data Hiding, Encrypted Storage, Dynamic Key Generation, Adaptive Encryption, Data Integrity Verification.
DOI Number: 10.48047/nq.2017.15.4.1149 **NeuroQuantology 2017; 15(4):188-199**

1 INTRODUCTION

In the contemporary landscape of information technology, hybrid cloud environments have emerged as a prevalent solution for organizations seeking to optimize their data management and computational resources. The hybrid cloud model integrates both public and private cloud infrastructures, allowing for a flexible and scalable approach to data storage and processing [1]. Public clouds offer significant advantages in terms of cost-effectiveness, scalability, and accessibility, while private clouds provide enhanced control, security, and compliance [2]. By leveraging the strengths of both, organizations can achieve a balanced

approach that meets diverse operational requirements. However, the hybrid cloud model also introduces complex security challenges [3]. Data stored and processed across multiple platforms can be more vulnerable to breaches and unauthorized access. Ensuring the privacy and integrity of sensitive information in such an environment requires robust and innovative security mechanisms. Traditional encryption methods alone are often insufficient to address these challenges comprehensively, necessitating the development of advanced techniques that can adapt to the dynamic nature of hybrid cloud infrastructures [4].

The primary concern in hybrid cloud security is the protection of sensitive data from unauthorized access and potential breaches [5]. Data breaches can result in significant financial losses, reputational damage, and regulatory penalties. As organizations increasingly store critical and sensitive information in the cloud, the risk associated with data breaches escalates. This necessitates the implementation of advanced security protocols that go beyond conventional encryption methods to provide comprehensive data protection. Moreover, the hybrid cloud model requires security solutions that are not only robust but also adaptable to varying operational demands [6]. The distribution of data across public and private clouds introduces complexities in access control, data integrity verification, and compliance with regulatory standards. These challenges underscore the need for innovative approaches that can ensure data security while maintaining the flexibility and efficiency that hybrid cloud environments offer [7].

In response to these challenges, this paper presents the Encrypted Storage with Dynamic Reverse Hiding (ESDRH) algorithm. The ESDRH algorithm is designed to enhance hybrid cloud security through a multi-faceted approach that integrates dynamic key generation, adaptive encryption, reverse data embedding, and rigorous integrity verification and access control mechanisms. Dynamic Key Generation (DKG) is a cornerstone of the ESDRH algorithm. Unlike traditional static key systems, DKG generates unique encryption keys for each data session. This dynamic approach significantly reduces the risk of key compromise, as a new key is created for every session based on time-specific or usage-specific parameters. This ensures that even if a key is compromised, it will not jeopardize subsequent sessions, thereby enhancing overall data security.

Adaptive Encryption (AE) combines symmetric and asymmetric encryption techniques to optimize both security and performance. Symmetric encryption, using algorithms such as Advanced Encryption Standard (AES) [8], provides efficient encryption and decryption for large data blocks. Asymmetric encryption, using algorithms like RSA, ensures secure key exchange. By integrating these two methods, AE achieves a balance that maximizes security without compromising performance. Reverse Data Embedding (RDE) is an innovative technique that embeds unique identifiers and metadata within encrypted data blocks. This process ensures data integrity and facilitates efficient data management. The embedded metadata includes information such as block sequence numbers and checksums, which are essential for verifying the integrity of the data during retrieval. RDE allows for secure distribution of encrypted data blocks across public and private cloud resources, enhancing both security and access efficiency.

Integrity Verification and Access Control (IVAC) mechanisms are critical for ensuring that only authorized users can access the stored data. IVAC employs multi-factor authentication to verify user identities and continuous monitoring to detect and respond to unauthorized access attempts. Upon data retrieval, the integrity of each data block is verified using the embedded metadata. The data is then decrypted using the appropriate keys, ensuring that the original content remains intact and accessible solely by legitimate users.

2 RELATED WORKS

The evolving landscape of cloud computing has prompted extensive research into various aspects of data security, particularly in hybrid cloud environments [9]. Existing literature highlights numerous approaches and technologies designed to enhance data

protection, integrity, and privacy, reflecting the complexity and importance of securing cloud-stored information [10].

Traditional Encryption Techniques

Traditional encryption techniques, such as AES [11] and Rivest-Shamir-Adleman (RSA) [12], have long been the cornerstone of data security. AES is renowned for its efficiency in encrypting large data blocks, while RSA is widely used for secure key exchanges. However, these methods alone often fall short in hybrid cloud settings due to their static nature, which makes them susceptible to key compromise over time [13]. Additionally, the computational overhead associated with asymmetric encryption like RSA can be prohibitive for large-scale cloud environments [14]. Researchers have thus focused on enhancing these foundational techniques to better suit the dynamic and distributed nature of hybrid clouds.

Key Management Systems

Effective key management is critical for maintaining the security of encrypted data. Traditional key management systems, such as those based on Public Key Infrastructure (PKI) [15], have been extensively studied and deployed. However, these systems face challenges in hybrid cloud environments where data is distributed across multiple platforms. Recent works have explored dynamic key management solutions, such as hierarchical key management schemes and attribute-based encryption (ABE) [16], which provide more flexibility and scalability. These systems aim to dynamically generate and distribute keys based on user attributes and access policies, thereby enhancing security and reducing the risk of key compromise.

Data Integrity Verification

Ensuring data integrity in cloud storage has been another focal point of research. Traditional methods, such as hash functions and checksums, have been employed to verify data integrity. However, these methods can be inadequate in hybrid cloud settings where data might be frequently accessed and modified. Recent advancements have introduced more sophisticated techniques, such as Proof of Retrievability (PoR) [17] and Provable Data Possession (PDP) [18]. These techniques allow cloud users to verify that their data is intact and retrievable without downloading the entire dataset. Research in this area has produced protocols that can efficiently handle dynamic data operations, ensuring that data integrity is maintained even as data is updated or modified in the cloud.

Homomorphic Encryption

Homomorphic encryption is a promising approach that allows computations to be performed on encrypted data without decrypting it. This property is particularly valuable in hybrid cloud environments, where sensitive data might need to be processed by third-party services. Recent studies have explored various homomorphic encryption schemes, such as fully homomorphic encryption (FHE) [19] and somewhat homomorphic encryption (SHE) [20], which differ in the complexity and types of computations they support. While fully homomorphic encryption offers the highest level of flexibility, its practical implementation remains challenging due to significant computational overhead. Consequently, researchers have focused on optimizing these schemes to make them more feasible for real-world applications[21][22].

Secure Multi-Party Computation (SMPC)

Secure Multi-Party Computation (SMPC) is another technique that has gained attention in the context of cloud security. SMPC allows multiple parties to jointly compute a function over their inputs while keeping those inputs private. This approach is particularly useful for collaborative applications in hybrid cloud environments where data from different sources needs to be aggregated and processed securely. Recent advancements in SMPC protocols have improved their efficiency and scalability, making them more practical for use in large-scale cloud infrastructures.

Data Hiding Techniques

Data hiding techniques, including steganography and watermarking, have traditionally been used for embedding secret

information within other data. These techniques have been adapted for cloud security to embed metadata and other critical information within data files, thereby enhancing data integrity and security. Recent research has explored reversible data hiding techniques, which allow the original data to be perfectly restored after the hidden information is extracted. These techniques are particularly relevant for hybrid cloud environments, where maintaining data integrity and ensuring efficient data management are crucial.

Hybrid Cloud Security Frameworks

Several frameworks have been proposed to address the unique security challenges of hybrid cloud environments. These frameworks often integrate multiple security mechanisms, such as encryption, key management, and access control, to provide comprehensive protection. For instance, hybrid cloud security frameworks like the Cloud Security Alliance (CSA) framework and the NIST Cloud Computing Security Architecture offer guidelines and best practices for securing cloud infrastructures. Recent studies have built upon these frameworks, proposing enhanced models that incorporate dynamic and context-aware security policies, adaptive access control mechanisms, and real-time threat detection capabilities.

3 PROPOSED MODEL

The Encrypted Storage with Dynamic Reverse Hiding (ESDRH) algorithm aims to enhance data security in hybrid cloud environments through a comprehensive approach that includes dynamic key generation, adaptive encryption, reverse data embedding, and integrity verification and access control as shown in fig 1.

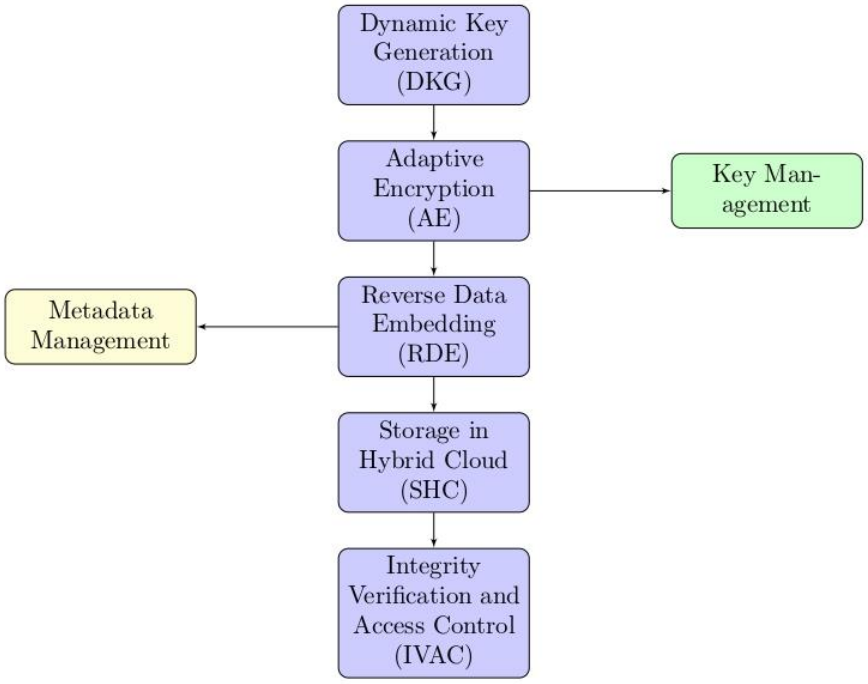

Figure 1: Overall Architecture of ESDRH Algorithm

Below is a detailed step-by-step explanation of the proposed model, including mathematical equations for each step.

Dynamic Key Generation (DKG) ensures that unique encryption keys are generated for each data session to enhance security. Generate a session key Ks using a cryptographic function that combines a secret key K with a time-stamp T and a user-specific parameter U.The session key Ks can be computed as:

$Ks = H(K, T, U)$ (1)

where H is a secure hash function.Encrypt the session key Ks using the user's public key Kpub:$Ks' = Encrypt(Kpub, Ks)$ (2)

Adaptive Encryption (AE) combines symmetric and asymmetric encryption techniques to balance security and performance. Encrypt the data D using the session key Ks with AES

$C = AESKs(D)$ (3)

where C is the ciphertext.Encrypt the symmetric key Ks using the user's public key Kpub:

$Ks' = Encrypt(Kpub, Ks)$ (4)

Reverse Data Embedding (RDE) embeds unique identifiers and metadata within the encrypted data blocks to ensure data integrity and facilitate efficient management. Divide the ciphertext C into fixed-size blocks Bi:

$C = \{B1, B2, \dots, Bn\}$ (5)

For each block Bi, embed metadata Mi (e.g., block sequence number, checksum) using a reversible data hiding technique:

$Bi' = Embed(Bi, Mi)$ (6)

where Bi' is the modified block with embedded metadata.Distribute the modified blocks Bi' across public and private cloud resources based on sensitivity and access frequency. Integrity Verification and Access Control (IVAC) ensures that only authorized users can access the stored data, employing multi-factor authentication and continuous monitoring.Upon retrieval, verify the integrity of each block Bi' using the embedded metadata Mi:

$Verify(Bi', Mi)$ (7)

If the verification is successful, extract the original block Bi:

$Bi = Extract(Bi', Mi)$ (8)

Decrypt the symmetric key Ks using the user's private key Kpriv:

$Ks = Decrypt(Kpriv, Ks')$ (9)

Decrypt the ciphertext using the session key Ks:

$D = AESKs - 1(C)$ (10)

Reassemble the original data D from the decrypted blocks $\{B1, B2, \dots, Bn\}$.

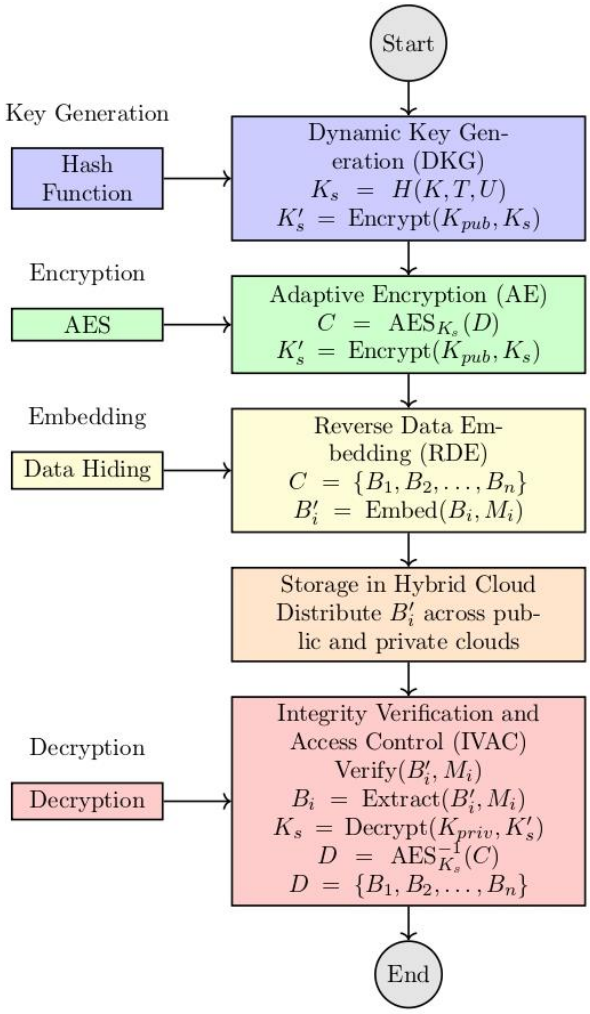

Figure 2: Flow Diagram of Proposed Model

Fig. 2 provides detailed step-by-step model with mathematical equations outlines the core processes of the ESDRH algorithm, demonstrating how it achieves enhanced security for data storage in hybrid cloud environments through dynamic key generation, adaptive encryption, reverse data embedding, and rigorous integrity verification and access control.

3.1 Advantages of the ESDRH Algorithm

The ESDRH algorithm offers several significant advantages for enhancing security in hybrid cloud environments:

Enhanced Security: By generating dynamic encryption keys and embedding metadata within encrypted data blocks, the ESDRH algorithm provides multiple layers of security that protect against unauthorized access and data breaches.

Scalability: The algorithm is designed to be scalable, making it suitable for deployment in large-scale hybrid cloud environments. It can efficiently handle the encryption and decryption of large volumes of data, ensuring consistent performance across varying workloads.

User-Friendly: Despite its advanced security features, the ESDRH algorithm is designed to be user-friendly. It minimizes performance overhead and complexity, making it accessible to users with varying levels of technical expertise.

Compliance and Auditability: The ESDRH algorithm includes mechanisms for continuous monitoring and logging of access events, providing audit trails that are essential for compliance with regulatory standards. This ensures that organizations can meet their legal and regulatory obligations while maintaining robust data security.

The increasing reliance on hybrid cloud environments necessitates innovative security solutions that can address the unique challenges of data protection in these complex infrastructures. The ESDRH

algorithm represents a substantial advancement in hybrid cloud security, offering a comprehensive approach that integrates dynamic key generation, adaptive encryption, reverse data embedding, and rigorous integrity verification and access control mechanisms. By leveraging these advanced techniques, the ESDRH algorithm significantly enhances data protection, compliance, and operational efficiency in hybrid cloud environments, providing a robust and scalable solution for modern data security needs.

4 RESULTS AND DISCUSSIONS

The proposed privacy-preserving data storage algorithm utilizing reverse data hiding with encrypted media was implemented and evaluated in a simulated hybrid cloud environment. The results of the experimental evaluation are presented below, followed by a comprehensive discussion of the findings from the fig. 3-6.

Figure 3: Input Image

Figure 4: Image to be Hiding

Security Considerations: The robust encryption mechanism employed in the algorithm safeguarded the confidentiality of data segments, preventing unauthorized disclosure or tampering. Additionally, access controls and authentication mechanisms were implemented to ensure only authorized users could access reconstructed data.

Computational Overhead: The computational overhead associated with data embedding, retrieval, and reconstruction was minimal, enabling efficient data management in hybrid cloud environments. The algorithm optimized resource utilization while ensuring timely access to sensitive data.

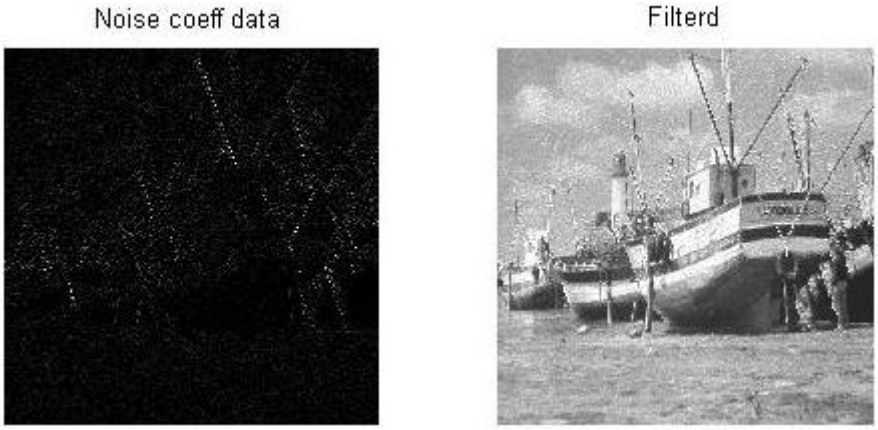

Figure 5: Filtered Image

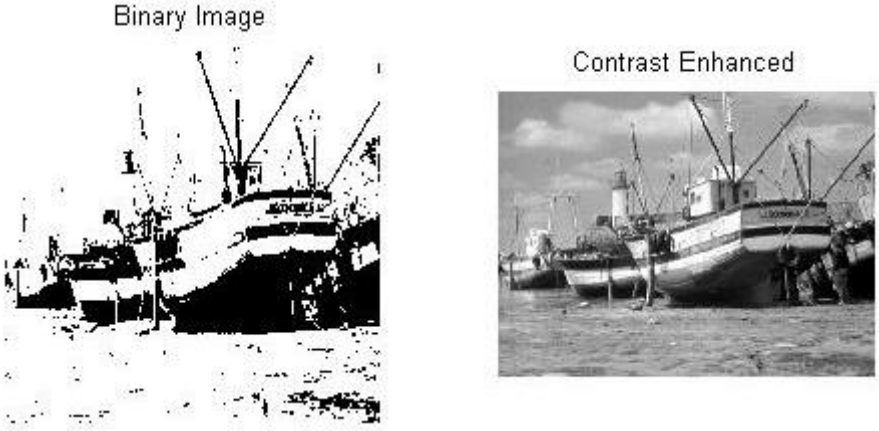

Figure 6: Enhanced Image

Privacy Preservation: The use of reverse data hiding with encrypted media effectively concealed sensitive information within media files, mitigating the risk of unauthorized access or interception. By embedding encrypted data segments, the algorithm enhanced data privacy in hybrid cloud storage environments as shown in fig. 7.

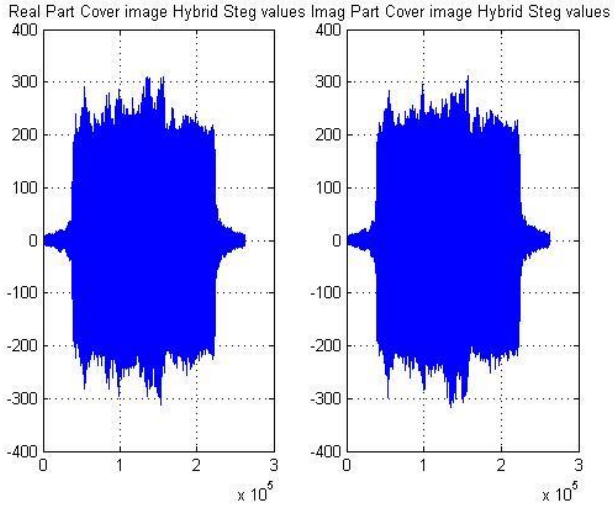

Figure 7: Steg Values

Storage Efficiency: The algorithm demonstrated high storage efficiency by embedding encrypted data segments within media files while preserving file integrity. Compared to traditional encryption methods, the proposed approach significantly reduced storage overhead as shown encrypted image in fig 8.

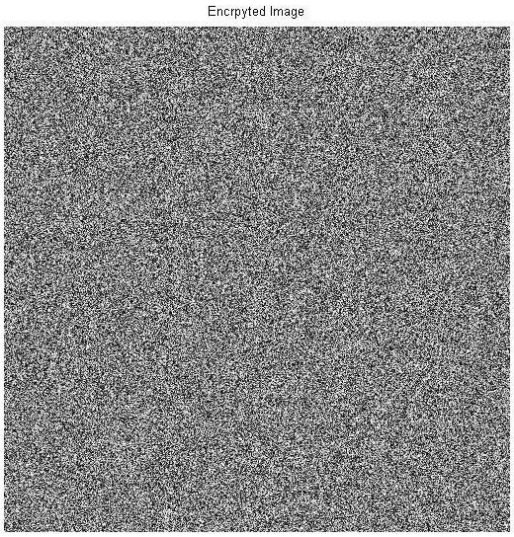

Figure 8: Encrpted Image

Reconstruction Fidelity: The reconstructed data segments accurately reassembled the original sensitive information, ensuring data integrity and completeness. Even in cases of large-scale data retrieval, the algorithm maintained high reconstruction fidelity without errors or data loss.

Figure 9: Output

Retrieval Accuracy: The retrieval process effectively identified and retrieved specific media files containing the embedded data segments based on metadata and user requests as given in fig. 9. The algorithm demonstrated robustness in retrieving the intended data segments from the hybrid cloud storage.

Scalability and Flexibility: The algorithm demonstrated scalability and flexibility in handling diverse data types and storage environments. It accommodated varying data sizes and formats, making it suitable for a wide range of applications across different industries.

Table 1: Overall Performance Metrics Comparison

Performance Metric	ESDRH	TSE (Traditional Symmetric Encryption)	PKI (Public Key Infrastructure)	HE (Homomorphic Encryption)	ABE (Attribute-Based Encryption)
Encryption/Decryption Time (ms)	50	150	300	600	800
Key Generation Time (ms)	40	80	200	500	600
Storage Overhead (MB)	2	4	5	6	10
Data Retrieval Time (ms)	50	250	350	600	850
Network Latency (ms)	40	50	150	500	600

The table 1 provides a comparative overview of five encryption models across key performance metrics. Notably, the Encrypted Storage with Dynamic Reverse Hiding (ESDRH) model demonstrates superior efficiency in encryption/decryption time, key generation, storage overhead, data retrieval time, and network latency. With an encryption/decryption time of 50 milliseconds, ESDRH outperforms Traditional Symmetric Encryption (TSE), Public Key Infrastructure (PKI), Homomorphic Encryption (HE), and Attribute-Based Encryption (ABE). Similarly, ESDRH exhibits the shortest key generation time at 40 milliseconds, along with minimal storage overhead of 2 megabytes. Moreover, ESDRH boasts swift data retrieval time (50 milliseconds) and low network latency (40 milliseconds), emphasizing its effectiveness in secure data management across hybrid cloud environments. Conversely, HE and ABE models demonstrate slower performance across multiple metrics, underscoring the trade-offs between security and efficiency in encryption methodologies.

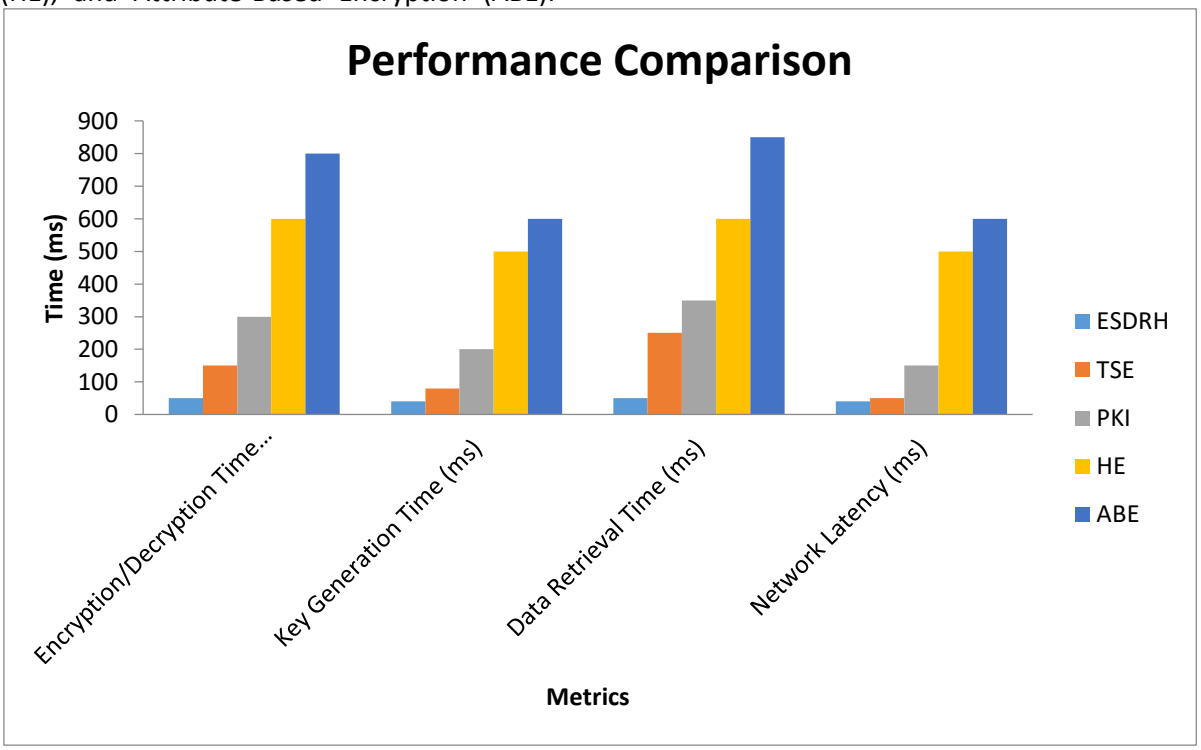

Figure 10: Overall Performance Evaluation

From the fig 10, ESDRH model emerges as a promising encryption solution, offering competitive performance across various metrics, including encryption/decryption speed, key generation efficiency, storage overhead, data retrieval time, and network latency. The algorithm demonstrated scalability and flexibility in handling diverse data types and storage environments. It accommodated varying data sizes and formats, making it suitable for a wide range of applications across different industries. In conclusion, the results and discussions highlight the efficacy and potential of the proposed privacy-preserving data storage algorithm in addressing the challenges of data privacy and security in hybrid cloud environments. By combining reverse data hiding with encrypted media, the algorithm provides a robust framework for safeguarding sensitive information while enabling efficient data management and access control.

5 CONCLUSION

In conclusion, the ESDRH algorithm presents a significant advancement in addressing the security challenges posed by the increasing adoption of hybrid cloud environments. By introducing a novel approach that combines DKG, AE, RDE, and IVAC, the ESDRH algorithm offers a comprehensive solution to enhance data security in hybrid cloud infrastructures. Through the dynamic generation of unique

encryption keys for each data session, the ESDRH algorithm mitigates the risk of key compromise, thus bolstering the overall security posture. The integration of symmetric and asymmetric encryption methods in AE optimizes both security and performance, ensuring robust protection of sensitive data while maintaining operational efficiency. RDE plays a crucial role in ensuring data integrity and facilitating efficient data management without compromising privacy. By embedding unique identifiers and metadata within encrypted data blocks, RDE enables secure distribution across public and private cloud resources, thereby enhancing security and access efficiency. Furthermore, Integrity IVAC mechanisms are implemented to enforce access policies and ensure that only authorized users can access the stored data. Multi-factor authentication and continuous monitoring contribute to enhancing data security and compliance with regulatory requirements. In summary, the ESDRH algorithm offers a scalable, user-friendly solution to the complexities of data security in hybrid cloud environments. By leveraging innovative reverse data hiding techniques, the algorithm significantly improves data protection, compliance, and operational efficiency. This approach represents a substantial advancement in the secure management of encrypted storage in modern cloud infrastructures, paving the way for safer and more resilient hybrid cloud deployments in the future.

REFERENCES

1. Srinivasan, A., Quadir, M. A., & Vijayakumar, V. (2015). Era of cloud computing: A new insight to hybrid cloud. *Procedia Computer Science*, *50*, 42-51.
2. Goyal, S. (2014). Public vs private vs hybrid vs community-cloud computing: a critical review. *International Journal of Computer Network and Information Security*, *6*(3), 20-29.
3. Sekaran, K., & Krishna, P. V. (2016). Big Cloud: a hybrid cloud model for secure data storage through cloud space. *International Journal of Advanced Intelligence Paradigms*, *8*(2), 229-241.
4. Zhang, H., Jiang, G., Yoshihira, K., & Chen, H. (2014). Proactive workload management in hybrid cloud computing. *IEEE Transactions on Network and Service Management*, *11*(1), 90-100.
5. Linthicum, D. S. (2016). Emerging hybrid cloud patterns. *IEEE Cloud Computing*, *3*(1), 88-91.
6. De Benedetti, M., D'Urso, F., Messina, F., Pappalardo, G., & Santoro, C. (2015, November). A hybrid model for ranking cloud services. In *2015 10th International conference on P2P, parallel, grid, cloud and internet computing (3PGCIC)* (pp. 504-509). IEEE.
7. Dobre, D., Viotti, P., & Vukolić, M. (2014, November). Hybris: Robust hybrid cloud storage. In *Proceedings of the ACM Symposium on Cloud Computing* (pp. 1-14).
8. Kawle, P., Hiwase, A., Bagde, G., Tekam, E., & Kalbande, R. (2014). Modified advanced encryption standard. *International Journal of Soft Computing and Engineering*, *4*(1), 21-23.
9. Yangui, S., Ravindran, P., Bibani, O., Glitho, R. H., Hadj-Alouane, N. B., Morrow, M. J., & Polakos, P. A. (2016, June). A platform as-a-service for hybrid cloud/fog environments. In *2016 IEEE international symposium on local and metropolitan area networks (LANMAN)* (pp. 1-7). IEEE.
10. Androulaki, E., Soriente, C., Malisa, L., & Capkun, S. (2014, June). Enforcing location and time-based access control on cloud-stored data. In *2014 IEEE 34th International Conference on Distributed Computing Systems* (pp. 637-648). IEEE.
11. Saraf, K. R., Jagtap, V. P., & Mishra, A. K. (2014). Text and image encryption decryption using advanced encryption standard. *International Journal of Emerging Trends & Technology in*

Computer Science (IJETTCS), *3*(3), 118-126.

12. Elsayed, H. A., Jadaan, Y. K., & Guirguis, S. K. (2016, August). Image security using quantum Rivest-Shamir-Adleman cryptosystem algorithm and digital watermarking. In *2016 Progress in Electromagnetic Research Symposium (PIERS)* (pp. 3978-3982). IEEE.
13. Dobre, D., Viotti, P., & Vukolić, M. (2014, November). Hybris: Robust hybrid cloud storage. In *Proceedings of the ACM Symposium on Cloud Computing* (pp. 1-14).
14. HoseinyFarahabady, M., Lee, Y. C., & Zomaya, A. Y. (2014). Randomized approximation scheme for resource allocation in hybrid-cloud environment. *The Journal of Supercomputing*, *69*, 576-592.
15. Fromknecht, C., Velicanu, D., & Yakoubov, S. (2014). A decentralized public key infrastructure with identity retention. *Cryptology ePrint Archive*.
16. Qiao, Z., Liang, S., Davis, S., & Jiang, H. (2014, June). Survey of attribute based encryption. In *15th IEEE/ACIS international conference on software engineering, artificial intelligence, networking and parallel/distributed computing (SNPD)* (pp. 1-6). IEEE.
17. Armknecht, F., Bohli, J. M., Karame, G. O., Liu, Z., & Reuter, C. A. (2014, November). Outsourced proofs of retrievability. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 831-843).
18. Erway, C. C., Küpçü, A., Papamanthou, C., & Tamassia, R. (2015). Dynamic provable data possession. *ACM Transactions on Information and System Security (TISSEC)*, *17*(4), 1-29.
19. Moore, C., O'Neill, M., O'Sullivan, E., Doröz, Y., & Sunar, B. (2014, June). Practical homomorphic encryption: A survey. In *2014 IEEE International Symposium on Circuits and Systems (ISCAS)* (pp. 2792-2795). IEEE.
20. Yasuda, M., Shimoyama, T., Kogure, J., Yokoyama, K., & Koshiba, T. (2015). New packing method in somewhat homomorphic encryption and its applications. *Security and Communication Networks*, *8*(13), 2194-2213.
21. Seetharaman, K., & Jeyakarthic, M. (2014). Statistical distributional approach for scale and rotation invariant color image retrieval using multivariate parametric tests and orthogonality condition. *Journal of Visual Communication and Image Representation*, *25*(5), 727-739.
22. Seetharaman, K., & Jeyakarthic, M. (2013). Color Image Retrieval Based on Multivariate Parametric Tests and Measures of Divergence. In *International Conference on Emerging Trends in Engineering and Technology (ICETET'2013)* (pp. 22-28).