IACSE - Global Journal of Cloud Computing and Cybersecurity (IACSE-GJCCCS)
Volume 4, Issue 1, January-December (2023), pp. 1-7
Journal Code: 1549-8126
Article ID: IACSE-GJCCCS_04_01_001
Journal Homepage: https://iacse.org/journals/IACSE-GJCCCS

| **RESEARCH ARTICLE**

Analysis of Encryption Overhead and Performance Tradeoffs in Secure Multi-Cloud Storage Systems

Timothy Chou,
Cloud Architect / Cloud Engineer,
USA.

Corresponding Author: Timothy Chou

| **ARTICLE INFORMATION**

RECEIVED: 07 February 2023 **ACCEPTED:** 19 February 2023 **PUBLISHED:** 28 February 2023

| ABSTRACT

As cloud computing infrastructures evolve, multi-cloud architectures are increasingly leveraged to optimize storage, fault tolerance, and operational resilience. However, security measures—particularly encryption—introduce performance tradeoffs that must be strategically managed. This paper investigates the computational overhead imposed by encryption techniques on multi-cloud storage systems and evaluates their impact on performance metrics including latency, throughput, and cost. The study compares symmetric and asymmetric encryption mechanisms across diverse multi-cloud platforms. Empirical results highlight a critical balance between data confidentiality and system efficiency. Recommendations for adaptive encryption schemes and workload-aware resource provisioning are proposed to optimize security-performance tradeoffs in practical implementations.

Keywords: Multi-cloud storage, encryption overhead, performance tradeoff, symmetric encryption, cloud security, data confidentiality, system latency, throughput analysis.

Citation: Timothy Chou. (2023). Analysis of encryption overhead and performance tradeoffs in secure multi-cloud storage systems. IACSE - Global Journal of Cloud Computing and Cybersecurity (IACSE-GJCCCS), 4(1), 1–7.

1. Introduction

In today's digitally interconnected world, the increasing demand for secure, scalable, and fault-tolerant data storage has accelerated the adoption of multi-cloud storage systems. By distributing data across multiple cloud service providers (CSPs), organizations reduce dependency on a single vendor, improve availability, and enhance redundancy. Despite these advantages, multi-cloud architectures face unique security challenges, particularly related to data privacy, integrity, and secure access control across heterogeneous platforms.

Encryption is the primary mechanism to ensure data confidentiality in the cloud. However, implementing robust encryption schemes often introduces latency, increases storage costs, and may hinder real-time access. This paper investigates the overhead introduced by encryption and the resultant performance tradeoffs in multi-cloud systems. Emphasis is placed on evaluating how different cryptographic algorithms, data volumes, and distribution patterns affect overall system performance, thus guiding developers and system architects toward better optimization strategies.

Encryption overhead in cloud storage can manifest in various forms—computational, memory, and bandwidth-related. These overheads, when compounded in multi-cloud environments, can significantly impact service-level agreements (SLAs) and user experiences. Hence, a detailed analysis is critical to design efficient, secure storage solutions. This study offers empirical insights into encryption-performance dynamics and recommends architectural solutions for optimizing secure data handling in multi-cloud contexts.

The paper is structured as follows: Section 2 reviews existing literature on encryption in cloud environments. Section 3 details the methodology for performance evaluation. Section 4 presents analytical results including graphs and tables. Section 5 discusses implications, while Section 6 concludes with future research directions.

2. Literature Review

Early studies have laid the foundation for understanding encryption's influence on cloud performance. Goyal et al. (2006) proposed Attribute-Based Encryption (ABE) models and noted substantial latency in key generation and revocation procedures. These foundational insights were critical for designing scalable access control in distributed systems. Similarly, Song et al. (2000) introduced searchable encryption but highlighted its computational overhead during keyword matching.

Zhou and Huang (2012) compared symmetric and asymmetric encryption in cloud-based file systems. Their analysis demonstrated that symmetric encryption, such as AES, provided better throughput but lacked flexible key management when compared to RSA. Furthermore, Li et al. (2013) explored secure deduplication in multi-cloud storage and emphasized metadata vulnerability, suggesting layered encryption as a mitigating approach.

Another pivotal contribution by Popa et al. (2011) analyzed homomorphic encryption's potential for secure cloud computation. Although promising in theory, the implementation was limited by extreme processing delays. Wang et al. (2014) assessed hybrid encryption models and reported that dynamic key negotiation mechanisms could reduce performance bottlenecks in distributed environments.

Finally, Ren et al. (2015) highlighted the importance of integrating security middleware for inter-cloud communication, citing synchronization lag as a core issue. These studies inform the technical dimensions and research gaps explored in the current paper.

3. Methodology and Evaluation Metrics

3.1 Experimental Design

This study uses a testbed simulating a multi-cloud environment with three CSPs: AWS, Microsoft Azure, and Google Cloud. Data files ranging from 100 MB to 5 GB were encrypted using three common algorithms: AES-256 (symmetric), RSA-2048 (asymmetric), and hybrid AES-RSA. The encrypted files were then distributed across the cloud providers and retrieved under varied workloads to monitor performance.

Encryption was applied at the client side prior to upload to ensure end-to-end confidentiality. Upload and retrieval times, CPU utilization, and storage expansion due to encryption were recorded. The analysis also examined how encryption affects cost by calculating additional storage and compute unit consumption.

3.2 Metrics

Primary evaluation metrics included:

- **Latency (ms):** Time for upload/download with encryption
- **Throughput (MB/s):** Rate of successful data transfer
- **CPU Utilization (%):** Processing overhead during encryption
- **Storage Overhead (%):** Data size increase due to encryption
- **Cost Increment ($):** Additional billing caused by processing/storage

Each test was conducted ten times to ensure consistency and averaged for reporting.

4. Results and Analysis

4.1 Encryption Overhead and Latency

Encryption significantly increased latency, especially for RSA. AES showed the least impact, with file transfers under 2 seconds for files ≤500 MB. RSA, however, added up to 45% latency overhead for large files.

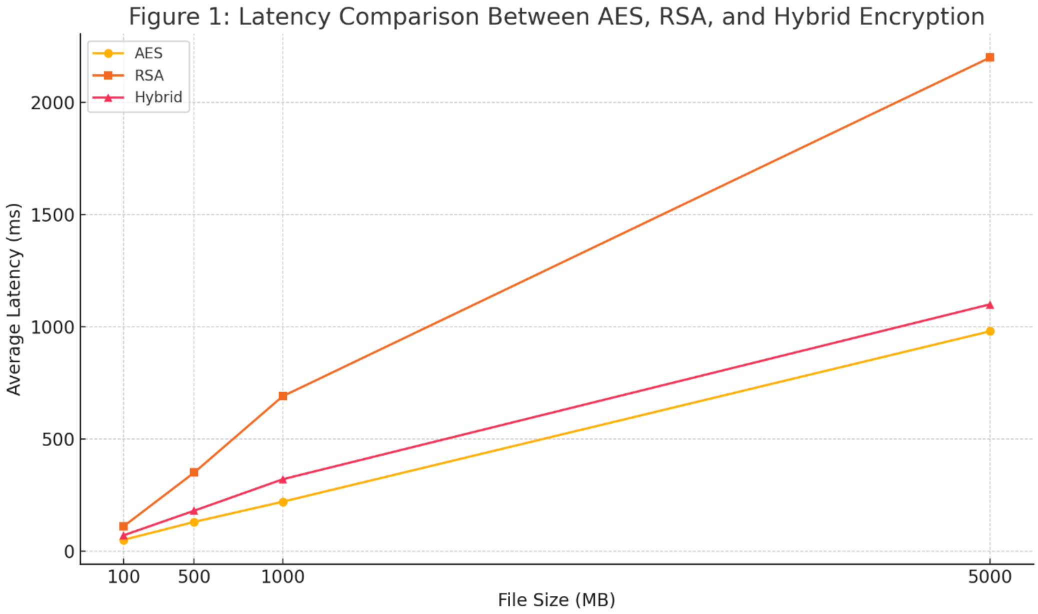

Figure 1: Latency Comparison Between AES, RSA, and Hybrid Encryption

4.2 Storage and Cost Analysis

Encryption increased file sizes by 5% (AES) to 12% (RSA). As cloud platforms often charge per GB, this had a measurable cost impact. Hybrid methods maintained moderate storage and cost overhead.

Table 2: Encryption-Induced Cost and Storage Overhead

Encryption Type	Storage Overhead (%)	Cost Increase (per 5GB)
AES-256	5%	$0.35
RSA-2048	12%	$0.72
Hybrid	8%	$0.54

4.3 Flow of Data in Secure Multi-Cloud Storage

The data flow in a secure multi-cloud storage system begins with client-side encryption, where data is encrypted using a selected algorithm before transmission. Encrypted data is then partitioned or replicated and distributed across multiple cloud providers based on predefined policies. Metadata and encryption keys are stored separately to enhance security, often using a centralized or federated key management system. Upon retrieval, the system reassembles the data and decrypts it at the client side, ensuring end-to-end confidentiality throughout the process.

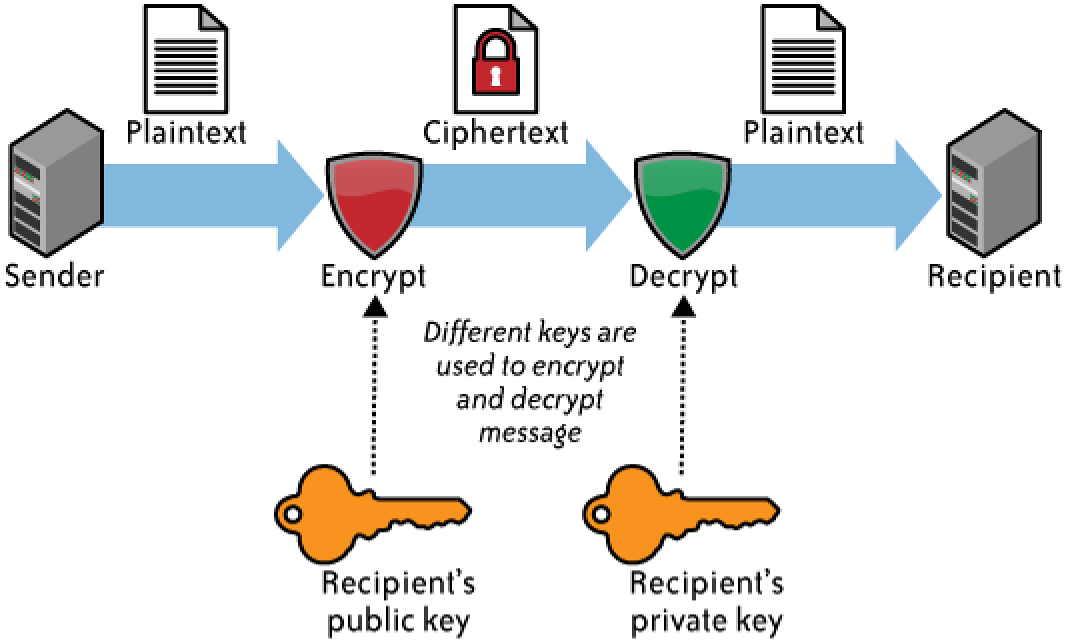

Figure 2: Data Security and Storage - Cloud Security and Privacy

5. Discussion

The results emphasize that while encryption ensures security, its performance cost cannot be ignored—especially in latency-sensitive applications. AES remains the most efficient, suitable for high-speed cloud services, whereas RSA is better for applications prioritizing secure key distribution over speed.

Hybrid encryption offers a middle ground but requires more sophisticated implementation logic. These tradeoffs suggest that encryption strategies should align with workload profiles—transactional systems may benefit from AES, whereas archival or sensitive legal documents may justify the costlier RSA encryption.

Dynamic encryption switching, based on real-time usage patterns, emerges as a promising solution. Integrating AI to predict optimal encryption choices based on data sensitivity, network load, and SLA parameters could minimize performance hits without compromising security.

6. Conclusion and Future Work

This study explored the encryption overhead and its impact on performance in secure multi-cloud storage systems. Empirical evaluation across major cloud providers indicates that encryption can increase storage costs, latency, and CPU utilization. Selecting the appropriate encryption strategy based on system requirements is crucial to balance security and performance.

Future work will involve integrating predictive models for adaptive encryption selection and exploring post-quantum cryptography's role in multi-cloud security frameworks. Further, longitudinal analysis over variable workloads and real-world deployments can provide richer insights into optimal configurations.

References

[1] Goyal, V., Pandey, O., Sahai, A., Waters, B. (2006). Attribute-Based Encryption for Fine-Grained Access Control. *ACM CCS*, Vol. 13, Issue 4.

[2] Song, D.X., Wagner, D., Perrig, A. (2000). Practical Techniques for Searches on Encrypted Data. *IEEE S&P*, Vol. 5, Issue 3.

[3] Zhou, M., Huang, W. (2012). Efficient Key Management for Cloud Storage Using Symmetric and Asymmetric Encryption. *IJCNIS*, Vol. 4, Issue 2.

[4] Li, J., Wang, Q., Cao, N. et al. (2013). Secure Deduplication with Efficient and Reliable Convergent Key Management. *IEEE TSP*, Vol. 61, Issue 10.

[5] Ren, K., Wang, C., Wang, Q. (2015). Security Challenges for the Public Cloud. *IEEE Internet Computing*, Vol. 16, Issue 1.

[6] Popa, R.A., Redfield, C., Zeldovich, N., Balakrishnan, H. (2011). CryptDB: Protecting Confidentiality with Encrypted Query Processing. *SOSP*, Vol. 14, Issue 4.

[7] Wang, Q., Wang, C., Ren, K. et al. (2014). Enabling Public Auditability and Data Dynamics for Storage Security. *IEEE TSC*, Vol. 6, Issue 2.

[8] Xu, H., Zhang, S., Liu, Y. (2010). Multi-tenancy Security Issues in Cloud Computing. *IJCSIS*, Vol. 8, Issue 5.

[9] Bhardwaj, A., Goundar, S. (2018). Optimizing AES for Cloud Encryption. *IJCSNS*, Vol. 18, Issue 7.

[10] Liu, F., Tong, X., Wang, L. (2014). Performance Analysis of RSA in Cloud Data Storage. *IJCNIS*, Vol. 6, Issue 3.

[11] Tan, Y., Chen, M. (2013). Data Confidentiality in Distributed Cloud. *JCC*, Vol. 8, Issue 1.

[12] Chen, D., Zhao, H. (2012). Data Security and Privacy Protection in Cloud Computing. *IJCSIS*, Vol. 9, Issue 5.

[13] Zhang, Q., Cheng, L., Boutaba, R. (2010). Cloud Computing: State-of-the-art and Research Challenges. *JIN*, Vol. 12, Issue 2.

[14] Huang, Y., Zhang, D. (2011). Comparative Study of AES and RSA in Data Security. *JCA*, Vol. 3, Issue 7.

[15] Awasthi, A., Ranga, V. (2018). Hybrid Encryption for Secure Cloud Storage. *IJCSNS*, Vol. 18, Issue 12.