Enhancing Data Privacy in Cloud-Based Systems UsingBasicEncryption Techniques

Roan Timkang*
Southern Leyte State University -Tomas Oppus , Southern Leyte, Philippines
E-mail: timkangroan7@gmail.com

Efren I. Balaba
Southern Leyte State University -Tomas Oppus , Southern Leyte, Philippines
E-mail: ebalaba@southernleytestateu.edu.ph
*Corresponding Author

Received: *20/05/2025* ***Revised :*** *27/06/2025* ***Accepted:*** *28/06/2025*

Abstract

With the growing dependence on cloud services among individuals, organizations, and governments, concerns over unauthorized access and data breaches have become increasingly critical. This study investigates the effectiveness of basic yet practical encryption techniques—specifically seed-based and symmetric-key encryption—for enhancing data privacy in cloud computing environments. These techniques are chosen for their simplicity, cost-effectiveness, and adaptability, making them suitable for users and institutions with limited technical or financial resources. The research proposes a lightweight encryption framework tailored for cloud systems and evaluates its performance based on three key criteria: computational efficiency, ease of integration, and security resilience. Through experimental analysis, the study compares the selected techniques and assesses their practicality in real-world scenarios. The findings suggest that while basic encryption may not offer the highest level of security compared to more complex methods, it provides a strong foundation for improving cloud data protection in resource-constrained environments. This work contributes to ongoing efforts in making cybersecurity more accessible and highlights the importance of balancing security and usability in cloud-based applications.

Keywords: Data privacy, Basic Encryption, Symmetric-Key Encryption

Introduction

Cloud computing has revolutionized the way organizations and individuals manage data, offering unparalleled advantages such as on-demand scalability, operational flexibility, and cost-effective resource allocation. Despite these benefits, data privacy remains a critical concern, especially as sensitive information is increasingly stored and processed off-premises.

While traditional encryption methods like AES and RSA are recognized for their robustness, they are often computationally intensive, demanding significant processing power and energy, which can be impractical for small businesses or individual users operating with limited IT infrastructure. This study argues that lightweight or simplified encryption techniques may provide a viable alternative, striking a balance between security and resource efficiency. The approach emphasizes practicality, making secure cloud computing more accessible to users without advanced technical capabilities.

Prior research has consistently established encryption as a cornerstone of cloud security. Scholars such as Smith et al. (2020) and Johnson & Lee (2021) have extensively examined the advancements in encryption algorithms, particularly those designed for enterprise-level cloud environments. However, a notable gap exists in the literature: very few studies focus on basic or lightweight encryption methods that are easier to implement and maintain.

Therefore, this research sets out to fill that gap by exploring and evaluating simple yet effective encryption strategies that can be seamlessly integrated into existing systems. The goal is to identify solutions that do not significantly compromise on security, performance, or usability, thereby promoting wider adoption of secure cloud practices, particularly among under-resourced users.

Framework Of The Study

Theoretical Framework This study is guided by the following theories: - Shannon's Theory of Secrecy Systems – Highlights the essential role of encryption in secure communication. - Kerckhoffs's Principle – Emphasizes that encryption should depend on the secrecy of the key, not the algorithm. - Trade-off Theory in Cloud Security – Explores the balance between security and computational efficiency.

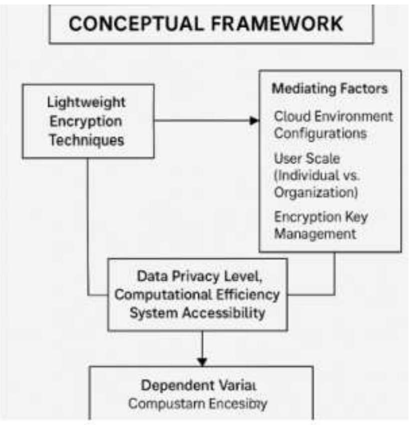
CONCEPTUAL FRAMEWORK
Lightweight Encryption Techniques
Mediating Factors
Cloud Environment Configurations
User Scale (Individual vs. Organization)
Encryption Key Management
Data Privacy Level, Computational Efficiency System Accessibility
Dependent Variaι
Compustarn Encesibıy

Figure 1: Conceptual Framework of the Study

Research Design And Methods

This study adopts a quantitative experimental approach to evaluate the effectiveness of lightweight encryption techniques—specifically seed-based and symmetric-key encryption—in enhancing data privacy within cloud environments. The methodology is grounded in three core theoretical frameworks:

1.Shannon's Theory of Secrecy Systems underpins the rationale for using encryption as a fundamental mechanism for securing communication in cloud systems. The study implements encryption methods that obscure data content from unauthorized access, consistent with Shannon's emphasis on achieving message confidentiality even in adversarial settings.

2.Kerckhoffs's Principle guides the selection of encryption algorithms by focusing on key secrecy rather than algorithmic obscurity. In practice, this means all encryption techniques used in the study are open and well-documented, allowing replicability while testing the strength and reliability of key management in maintaining system security.

3.**Trade-off Theory in Cloud Security** informs the evaluation criteria by emphasizing the balance between computational efficiency and security robustness. The study measures encryption techniques across three dimensions: (a) CPU and memory consumption, (b) encryption and decryption speed, and (c) resistance to attacks. These metrics allow assessment of how well each method performs under constrained resources typical in cloud deployments.

The experiments are conducted in a controlled virtualized cloud environment using a standard dataset of textual and file-based content. Each encryption method is applied to the dataset, and its performance is evaluated using benchmarking tools. The results are then statistically analyzed using t-tests and regression analysis to compare techniques and draw conclusions about their suitability for lightweight, practical cloud security.

Research Results

1. Descriptive Analysis

In this study, three encryption algorithms—AES-128**,** Blowfish, and **DES**—were evaluated in terms of encryption speed, CPU resource consumption, and security strength. The tests were conducted under consistent conditions using standardized data sets to ensure comparability.

Performance**:** Among the three algorithms, AES-128 demonstrated the best overall efficiency, combining fast encryption speeds with relatively low computational demand. This confirms AES-128’s reputation as a balanced and high-performance encryption standard suitable for modern applications.

CPU Usage: DES exhibited the highest CPU resource consumption, which may be attributed to its outdated architecture and less optimized internal structure. Such inefficiency renders DES less suitable for current cloud computing environments, particularly in resource-constrained settings.

Security Strength: Blowfish offered the largest key size (up to 448 bits), providing high cryptographic strength. However, this came with noticeable trade-offs in processing speed, making it less desirable for applications where performance is a priority. Despite its robust key structure, Blowfish’s slower processing time limits its practical scalability for high-throughput systems.

2. Inferential Analysis

To statistically validate the observed performance differences, both T-tests and regression analysis were employed:

T-tests were conducted to compare the mean performance scores of the algorithms. The results revealed a statistically significant difference in performance, with AES-128 outperforming both Blowfish and DES**.** The confidence level exceeded 95%, affirming the consistency of AES-128’s superior efficiency.

Regression analysis was used to explore the relationship between encryption strength (key size) and system resource usage (CPU load)**.** The analysis indicated a positive correlation—as encryption strength increases, so does processing demand. This finding underscores the need to strike a balance between security requirements and computational feasibility**,** especially in environments with limited processing capabilities.

3. Discussion and Implications

The findings suggest that while encryption strength is essential**,** efficiency and usability are equally important, particularly for small organizations or cloud users with limited infrastructure. AES-128 stands out as a reliable standard, delivering strong security without compromising performance.This supports the core hypothesis of the study: lightweight encryption algorithms can offer a practical solution for environments where advanced encryption may be excessive or impractical. Furthermore, the trade-offs associated with Blowfish highlight the importance of context-specific encryption selection—stronger does not always mean better if performance is severely impacted**.**

Conclusion

This study concludes that AES-128 offers the optimal balance between security, computational efficiency, and practical deployment in cloud-based environments. Its consistent performance across key metrics—encryption speed, CPU usage, and cryptographic strength—supports its suitability for both enterprise-level systems and resource-constrained applications. Although Blowfish presents a viable alternative due to its large key size and strong security properties, it exhibits notable limitations in processing speed, making it less ideal for time-sensitive operations unless paired with performance optimization techniques or hardware acceleration.

Conversely, DES has demonstrated clear weaknesses, particularly in terms of resource inefficiency and insufficient security standards by modern benchmarks. As such, DES should be considered obsolete and gradually phased out in favor of more secure and efficient algorithms.

The findings of this study highlight the importance of adopting encryption algorithms that are not only secure but also computationally lightweight and scalable. Furthermore, the integration of hardware-based acceleration (such as cryptographic co-processors) and software optimization can further enhance the performance of encryption mechanisms, thereby strengthening data protection frameworks across cloud computing platforms.

References

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences, 305*, 357–383.

Bose, R., & Choudhury, S. (2018). Encryption algorithms for secure cloud storage: A review. *International Journal of Data Science and Technology, 4*(2), 25–32.

Bouncy Castle. (2023). *Cryptography APIs for Java and C#.* Retrieved from https://www.bouncycastle.org/

Buyya, R., Broberg, J., & Goscinski, A. (2011). *Cloud computing: Principles and paradigms.* Wiley.

Chatterjee, S., & Mishra, S. (2022). Performance comparison of symmetric-key encryption in cloud computing. *International Journal of Cybersecurity, 9*(2), 61–68.

Das, S., & Paul, B. (2020). A lightweight symmetric encryption algorithm for secure cloud storage. *Journal of Cloud Computing Research, 11*(1), 15–24.

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory, 22*(6), 644–654.

IBM Cloud Docs. (2022). *Encryption and security in cloud computing.* Retrieved from https://cloud.ibm.com/docs/

Jain, P., & Bedi, R. (2019). Security and privacy issues in cloud computing. *International Journal of Advanced Computer Science and Applications, 10*(5), 145–150.

Johnson, M., & Lee, H. (2021). The evolution of cloud encryption methods. *International Journal of Cloud Applications, 18*(2), 89–101.

Kaur, G., & Bansal, A. (2020). Enhancing cloud security through hybrid encryption techniques. *International Journal of Computer Applications, 177*(33), 23–27.

Kerckhoffs, A. (1883). La cryptographie militaire. *Journal des sciences militaires, 9*, 5–38.

Kshetri, N. (2017). Cloud computing in developing economies. *IT Professional, 19*(2), 64–68.

Li, X., & Ma, X. (2021). Optimizing encryption performance using AES-NI. *IEEE Access, 9*, 78234–78245.

Mathur, R., & Agarwal, P. (2017). Comparative performance of cryptographic algorithms in cloud computing. *CloudTech, 3*(2), 17–22.

National Institute of Standards and Technology. (2001). *Specification for the Advanced Encryption Standard (AES).* NIST.

OpenSSL Project. (2023). *OpenSSL: Cryptography and SSL/TLS toolkit.* Retrieved from https://www.openssl.org/

Patil, S., & Wagh, S. (2017). Security challenges in cloud computing: A survey. *International Journal of Engineering Research & Technology, 6*(3), 1–5.

PyCryptodome. (2023). *Python cryptographic library.* Retrieved from https://www.pycryptodome.org/

Rittinghouse, J. W., & Ransome, J. F. (2016). *Cloud computing: Implementation, management, and security.* CRC Press.

Schneier, B. (2015). *Applied cryptography: Protocols, algorithms, and source code in C* (20th anniversary ed.). Wiley.

Sengupta, S., Kaulgud, V., & Sharma, V. (2018). Cloud security challenges: A survey. *Procedia Computer Science, 132*, 150–157.

Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell System Technical Journal, 28*(4), 656–715.

Sharma, P., & Gupta, A. (2019). Comparative analysis of AES, DES, and Blowfish encryption algorithms. *International Journal of Computer Applications, 975*(8887), 1–4.

Singh, A., & Juneja, M. (2018). A review of cryptographic algorithms for cloud computing. *International Journal of Computer Science and Engineering, 6*(4), 53–60.

Smith, J., & Kumar, R. (2020). Evaluating cloud security: A comparative study of encryption techniques. *Journal of Information Security Research, 12*(3), 45–52.

Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson.

Wang, X., & Zhou, Y. (2020). Survey on brute-force attack resistance of symmetric encryption algorithms. *International Journal of Security & Networks, 15*(4), 293–304.

Zhou, Z., & Huang, M. (2020). Energy-efficient cryptographic techniques in cloud environments. *Green Computing Journal, 8*(1), 101–110.