Adapting DES and AES Cryptography for Secure Cloud Computing Environments

Narendra Kumar and Leszek Ziora

NIET NIMS University, Jaipur, India

CUT Poland

ARTICLE INFO

Article History:

Received December 3, 2024

Revised December 18,2024

Accepted January 3, 2025

Available online January 18, 2025

Keywords:

AES,

cloud computing,

encryption,

decryption,

DES.

Correspondence:

E-mail: drnk.cse@gmail.com

ABSTRACT

Increased concern about data security is now experienced with cloud computing, mainly on the aspect of data confidentiality of the CSP. This research examines the use of cryptographic algorithms such as DES and AES in cloud computing to alleviate the security risk. Simulations in Matlab R2009a are conducted based on a quantitative approach for evaluating the encryption speed, data security, and the resource usage of both algorithms. Findings show that although DES improves data security, the short key length and susceptibility to cryptographic attacks make it less efficient for large-scale cloud applications. On the other hand, AES has better security and scalability but is hindered by its computational intensity. The comparative analysis suggests that AES is a better choice for cloud security if optimization strategies overcome its resource-intensive nature. It, therefore, contributes to understanding solutions in cryptographic secure cloud computing and emphasizes the need for tailored encryption standards that respond to specific cloud security needs. Future research should further address emerging cryptographic technologies and real-world implications for diverse cloud environments.

Introduction

This chapter discusses the growing trend of cloud computing and the associated increase in security issues, particularly data confidentiality with CSPs. The central research question addresses the issue of whether cryptographic algorithms, such as DES and AES, can reduce security risks in the cloud. Five sub-research questions will guide this investigation: How does DES enhance data security in cloud systems? What are the limitations of DES in cloud computing? How does AES improve upon DES for cloud data protection? What challenges does AES face in cloud environments? How do DES and AES compare in terms of performance, scalability, and resource consumption in cloud settings? The research uses a quantitative approach where Matlab R2009a is used for simulation purposes to evaluate the effects of these encryption standards on cloud security. The paper follows this outline: a literature review on cryptographic solutions, methodology on simulation procedures, results from testing algorithms, and a conclusion discussing the findings and implications for secure cloud computing.

- **DES Role in Strengthening Cloud Security**

Early work did focus on DES as an effective means for securing data in the cloud by utilizing a symmetric encryption mechanism. Yet these early works usually complained that DES is vulnerable to brute-force attacks, because it is relatively short and weak in key length. The next round of research targeted those weaknesses by proposing new versions of DES but somehow did not have a dynamic test for the new design in cloud environments. Recent studies emphasize the integration of DES with other security protocols, but there are still problems in scalability and performance. Hypothesis 1: DES significantly enhances data security in cloud systems, but its effectiveness is hampered by weaknesses in key length.

- **Limitations of DES in Cloud Computing**

Initial studies were more concerned with the speed of DES encryption and its ease of implementation, but these studies often neglected the fact that DES is vulnerable to some forms of cryptographic attacks, such as differential cryptanalysis. Subsequent researches tried to measure these weaknesses, and it was found that although DES provides satisfactory security for smaller data, it cannot handle large-scale, complex cloud environments. Current research focuses on the need for stronger, more flexible algorithms in the cloud. Hypothesis 2: The weakness of DES in cloud computing is due to its susceptibility to cryptographic attacks and inability to deal with big data securely.

- **AES's Advantages Over DES for Cloud Security**

Initial research indicated that AES is more secure than DES because of its longer key length and more complex encryption process. These studies showed that AES can stand against several attack vectors used to compromise DES. Mid-term research confirmed the security of AES by using real-world applications in cloud environments but with performance trade-offs on initial implementations. Current research focuses on optimizing AES for cloud computing, balancing between security and efficiency. Hypothesis 3: AES significantly improves cloud data security over DES, especially when it comes to cryptographic attacks.

- **Challenges with AES in Cloud Environments**

The first studies revolved around the implementation of AES in cloud systems and stated that AES is computation-intensive and will affect system performance. Further research then considered solutions for such negative impacts, including hardware acceleration and optimization techniques, which still lacked extensive evaluations of AES in different cloud infrastructures. Recent studies aim to balance AES's security benefits with its computational demands, yet challenges remain in achieving optimal performance without compromising security. Hypothesis 4: AES faces challenges in cloud environments due to its computational demands, necessitating optimization for efficient performance.

- **Comparative Analysis of DES and AES in Cloud Computing**

Initial comparisons between DES and AES focused on basic performance metrics, often highlighting AES's advantages in security and scalability. However, these researches often ignored real-time application scenarios and resource consumption issues. Subsequent research used more sophisticated simulations and demonstrated subtle variations in their performance across different cloud scenarios. The most recent research indicates that these algorithms have to be tested contextually to understand the trade-off between them. Hypothesis 5: DES and AES have significantly varying performance, scalability, and resource consumption with AES having a better security outcome for cloud computing scenarios.

Method

This section explains a quantitative research approach applied on assessing the efficiency of the DES and AES algorithms in cloud security, where data collection is done along with explaining variables adopted for the study. This helps understand the intense processes used in testing the said encryption standards.

Data

Data for this research are collected during simulations that were performed employing Matlab R2009a. The simulation considers the implementation and execution of DES and AES in cloud environments. Scenarios include different cloud computing scenarios to ensure a broad basis of security and performance characteristics. Sampling techniques include diverse instances of cloud service models or configurations. The criteria of the study centring on encryption speed, level of data security, and resource usage across different cloud infrastructures result in a detailed dataset capable of testing the efficiency of cryptographic algorithms.

Variables

Independent variables are type and key length and configurations regarding the encryption algorithm (DES and AES). Dependent variables are the performance metrics centred on encryption speed, security level, and the quantity of resources consumed. Instrumental variables are cloud environment configuration and computational resources provision for encryption processes. Control variables are network conditions and data volume so that the analysis can remove extraneous effects of encryption algorithms on cloud security. Literature from cryptography and cloud computing research is used to substantiate the measurement methods for such variables, thus guaranteeing reliability and accuracy of results.

Results and Discussion

This section critically assesses the existing literature that addresses DES and AES encryption standards in cloud environments, focusing on the sub-research questions developed in the introduction. It discusses the effectiveness and limitations of both algorithms, comparing their performances and security implications in a cloud environment. This section also summarizes some of the deficiencies of past work, which include underemphasis on real-time applicability and lack of scalability, and discusses how this paper will bridge these gaps. The section concludes with five hypotheses relating encryption algorithms to cloud security, that are tested in subsequent sections.

Results It depicts an all-inclusive study on the performance and security implication of DES and AES encryption algorithms in cloud computing using data from Matlab R2009a simulations. The descriptive statistical analysis portrays an overview of encryption speed, data security, and consumption of resources for the two algorithms. Regression analysis supports the hypotheses by clearly proving the superiority of AES, where it offers solid security and handles larger data efficiently. However, the computational requirements of AES necessitate optimization to maintain system performance. The results emphasize the importance of choosing appropriate encryption standards based on specific cloud computing needs and security requirements. Effectiveness of DES in Cloud Security This finding confirms Hypothesis 1, which states that DES improves cloud data security due to its symmetric encryption mechanism. Analysis of simulation data indicates that DES effectively secures data against unauthorized access in controlled environments, with encryption speed being one of the advantages. The independent variables include the DES key length and configuration, while the dependent variables are security metrics such as encryption strength and data integrity. Empirical significance of DES in secure cloud applications resonates with classical encryption theories as it plays a fundamental role in securing data. Nevertheless, in large-scale applications, limitations in key length make security difficult, and it will also pose other requirements for additional security support. This finding thus depicts the need to balance security versus performance regarding DES, especially in cloud computing environments.

- **Overcoming DES Challenges in Cloud Computing**

This outcome supports Hypothesis 2, which says DES is limited in cloud computing due to its vulnerability towards cryptographic attacks and problems while dealing with large amounts of data securely. The simulation results indicated that DES is vulnerable to some attack vectors, especially in dynamic cloud environments where the data volume and complexity increase. Independent variables are key: they include the encryption configuration of DES, whereas dependent variables focus on vulnerability metrics, such as susceptibility to attacks and data breach incidents. Empirical significance implies that, though DES provides basic security, its application in the cloud is highly restricted because it cannot ensure effective security of large data. This suggests that high-grade encryption technologies need to be developed for overcoming such deficiencies and complete protection of data in the cloud.

- **The Findings for Hypothesis** 3

It indicates that AES provides more enhanced security over DES, protecting cloud data. Simulation data indicate robust security features provided by AES such as resistance to more ranges of cryptographic attacks and enhanced integrity. Independent variables in this model will be the AES key length and configuration, while dependent variables are on metrics about security, including the encryption strength and breach prevention. In empirical terms, this reflects AES's security capacities aligned with modern encryption theories in supporting its use within secure cloud applications. However, the analysis also shows performance trade-offs, which imply that optimization is required for maintaining system efficiency. This result indicates that advanced encryption standards are essential for securing cloud data and that AES is the preferred choice for secure cloud computing.

- **AES Challenges in Cloud Environments**

This result supports Hypothesis 4, which states that AES faces challenges in cloud environments due to its computational demands and needs optimization for efficient performance. Simulation results show that although AES offers better security, the implementation of AES may negatively affect system performance, especially in resource-constrained cloud environments. The independent variables are AES encryption configuration, while dependent variables focus on performance metrics, such as encryption speed and resource usage. Empirical significance suggests that optimizing AES for cloud environments is important in balancing security and efficiency with theories of computational optimization in encryption. This result points to the necessity of customized solutions for improving the applicability of AES in various cloud infrastructures while maintaining security robustness without degrading system performance.

- **Comparative Analysis of DES and AES Performance**

This result confirms Hypothesis 5, which states that there are significant differences between DES and AES in terms of performance, scalability, and resource consumption in cloud computing environments. Comparative analysis of simulation data shows that AES generally offers better security results, with better scalability and data protection. The independent variables are encryption algorithm type and configuration, while the dependent variables are performance metrics such as encryption speed, scalability, and resource efficiency. The empirical significance highlights the superiority of AES in handling complex cloud applications, which makes it a preferred encryption standard for secure cloud computing. Based on specific cloud security needs, different encryption algorithms should be employed to ensure optimal performance in light of that protection.

Conclusion

Through this research, the strengths of DES and AES for cryptography were given consideration along with their roles in improved data security and solutions regarding definite challenges in cloud environments. The results show AES performance is better than that offered by DES in terms of security and handling large chunks of data, though higher computational requirements call for better optimization. This research will enhance the knowledge of cryptographic solutions for secure cloud computing while providing insight into the selection of proper standards for encryption based on individual needs. However, reliance on simulation data may not capture real-world complexities; further research is also warranted in exploring emerging encryption technologies. Future research should involve an investigation of additional cryptographic solutions and their implications in diversified cloud settings to enhance best practices in secure cloud computing.children literature much like African adult literature is often socially didactic, ‗arts for life's sake' and as such encourages children to be good and to shun evil for the growth of a morally focused society because it is well known Abraka Humanities Review, Vol. 10 Num. 1, 2020 Abraka Humanities Review, Vol. 10 Num. 1, 2020 77 and widely believed that children are the future of any society, region and nation. This chapter therefore concludes that African children's prose fiction serves a major role in educating African children on African values. However, more can, and should be done in the production and promotion of prose fiction for the African children.

References

[1] Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice.* Pearson.

[2] Narendra Kumar, B. Srinivas and Alok Kumar Aggrawal: "Finding Vulnerabilities in Rich Internet Applications (Flex/AS3) Using Static Techniques-2" I. J. Modern Education and Computer Science, 2012, 1, 33-39.(http://www.mecs-press.org/ DOI: 10.5815/ijmecs.2012.01.05)

[3] Anuj Kumar, Narendra Kumar and Alok Aggrawal: "An Analytical Study for Security and Power Control in MANET" International Journal of Engineering Trends and Technology, Vol 4(2), 105-107, 2013.

[4] Anuj Kumar, Narendra Kumar and Alok Aggrawal: "Balancing Exploration and Exploitation using Search Mining Techniques" in IJETT, 3(2), 158-160, 2012

[5] Anuj Kumar, Shilpi Srivastav, Narendra Kumar and Alok Agarwal "Dynamic Frequency Hopping: A Major Boon towards Performance Improvisation of a GSM Mobile Network" International Journal of Computer Trends and Technology, vol 3(5) pp 677-684, 2012.

[6] Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* Wiley.

[7] Diffie, W., & Hellman, M. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22(6), 644–654.

[8] Daemen, J., & Rijmen, V. (2002). *The Design of Rijndael: AES - The Advanced Encryption Standard.* Springer.

[9] NIST. (2001). Advanced Encryption Standard (AES). *Federal Information Processing Standards Publication 197.*

[10] Kelsey, J., Schneier, B., Wagner, D., & Hall, C. (1997). Cryptanalytic Attacks on Pseudorandom Number Generators. *International Workshop on Fast Software Encryption*, 168–188.

[11] Ferguson, N., & Schneier, B. (2003). *Practical Cryptography*. Wiley.

[12] Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds. *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS)*, 199–212.

[13] Cloud Security Alliance (CSA). (2016). *Best Practices for Securing Cloud Applications.*

[14] Viega, J., & McGraw, G. (2001). *Building Secure Software: How to Avoid Security Problems the Right Way.* Addison-Wesley.

[15] Menezes, A., van Oorschot, P., & Vanstone, S. (1996). *Handbook of Applied Cryptography.* CRC Press.

[16] Singh, A., & Shrivastava, S. (2017). Overview of Attacks on Cryptographic Algorithms. *Journal of Information Security*, 8(1), 80–98.

[17] Song, D., Wagner, D., & Perrig, A. (2000). Practical Techniques for Searches on Encrypted Data. *IEEE Symposium on Security and Privacy*, 44–55.

[18] Wang, C., Ren, K., & Lou, W. (2010). Toward Publicly Auditable Secure Cloud Data Storage Services. *IEEE Network*, 24(4), 19–24.

[19] 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.