International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 March 2023 **Revised:** 12 April 2023 **Accepted:** 30 May 2023*

Evaluating the Efficacy and Security of Steganography Techniques in Cloud Computing

Apeksha Dave
Ph.D. Scholar
Department of Computer Application
Dr. A. P. J. Abdul Kalam University, Indore MP.
Email: apekshadave650@gmail.com

Dr. Sandeep Singh Rajpoot
Department of Computer Application
Dr. A. P. J. Abdul Kalam University, Indore MP.
Email: sandeepraj413@gmail.com

Abstract— Cloud computing has revolutionized the handling, access, and storage of data. However, ensuring the security and privacy of data within cloud environments remains a significant challenge. This research offers a comprehensive examination aimed at developing a dependable steganographic technique, evaluating its effectiveness, determining its impact on cloud computing performance, and exploring potential vulnerabilities along with solutions. The primary objective is to assess how steganography influences the performance of cloud computing systems. Through performance evaluations and benchmarks, the study investigates the effects of steganography on system performance. It utilizes various file formats and sizes to simulate real-world conditions. The research also identifies potential weaknesses of the proposed steganographic method and explores strategies to mitigate these vulnerabilities. An analysis of security vulnerabilities, including potential attacks and detection techniques, leads to the formulation of effective countermeasures. The findings of this research contribute to the advancement of steganography-based data security in cloud environments. By highlighting the strengths, weaknesses, and areas for improvement of the proposed steganographic approach, the study offers insights into its impact on cloud computing systems and supports the development of robust security measures.

Keywords: steganography, cloud computing, data security, Serpent encryption, performance evaluation, vulnerabilities, countermeasures.

I. INTRODUCTION

A basic paradigm for storing, analysing, and accessing enormous volumes of data is cloud computing. But maintaining the security and privacy of data in cloud settings is still a critical challenge. Traditional encryption methods by themselves could not offer enough defence against advanced attackers. A strategy that has promise for improving data security in cloud computing systems is steganography, the art of concealing information under harmless cover media. Steganography may provide another level of security and integrity to sensitive information by enclosing encrypted data in seemingly innocent files. The assessment of the effect of steganography on the functionality of cloud computing systems becomes the subject. This purpose intends to quantify the impact of steganography on computing resources, network bandwidth, and overall system performance through performance studies and benchmarks. To imitate real-world situations and provide light on the scalability and effectiveness of the suggested steganographic approach, several file kinds and sizes are used. Investigating possible weaknesses and defences in the suggested steganographic technique is one of the focus of this study . The purpose of this objective is to locate and evaluate security flaws that might jeopardise the steganographic technique's efficacy. Appropriate countermeasures may be developed to reduce these vulnerabilities and improve the overall security of the steganographic system by having a thorough awareness of prospective assaults and detection methods.

These goals will be addressed in this research endeavour, which intends to develop steganography-based data security in cloud computing settings. The research sheds light on the advantages, disadvantages, and possible areas for development of the suggested steganographic approach. Additionally, the performance assessment and vulnerability analysis help in the creation of efficient countermeasures to improve data security by fostering a thorough understanding of the effects of steganography on cloud computing systems.

2. Literature Review

Steganography and Cloud Computing Security:

In the area of data security, steganography, a method for concealing information within cover media, has received a lot of interest. A possible method to improve the security and secrecy of data stored and sent inside cloud computing settings is the use of steganography. For the purpose of preventing unauthorised access to and detection of sensitive data, several academics have investigated the integration of steganography with cloud computing.

A steganographic method that combines RSA encryption with data embedding in cloud storage systems was suggested in one important paper by Li et al. [1]. The authors highlighted the benefits of steganography in cloud contexts and showed how their technique effectively preserved data secrecy and integrity. Another research by Zhang et al. [2] presented a steganographic method that used distributed storage across several cloud servers and wavelet-based picture concealing. The authors' thorough testing of the method's security and performance facets revealed that it was resistant to assaults and had no effect on system performance.

Performance Evaluation in Steganography and Cloud Computing:

Analysing the performance impact becomes essential when steganography incorporation into cloud computing systems is being considered. This issue has been studied in research papers by measuring the computing resources and network bandwidth used by steganographic techniques in cloud settings through performance assessments and benchmarking.

The performance assessment of a steganographic technique in cloud computing systems was the topic of a study by Wang et al. [3]. The authors looked at how different file types and sizes affected system performance when data was embedded in them. Their research brought to light the tension between security and performance, highlighting the necessity of streamlining the steganographic procedure to prevent performance loss.

Vulnerabilities and Countermeasures in Steganography:

Steganography improves data security, but it's crucial to look for any weaknesses that can make it less effective. To find security flaws and provide defences against these dangers, researchers have performed studies. Chen et al.'s seminal study [4] examined possible steganography attacks on cloud computing platforms. Numerous attack routes, such as statistical analysis, ocular examination, and watermarking detection, were examined by the authors. They suggested remedies to strengthen the security of steganographic systems in the cloud, including encryption techniques and data fragmentation.

Steganography is important for strengthening data security in cloud computing environments, according to the literature study. Researchers have put forth steganographic approaches that combine data embedding with encryption algorithms to protect the secrecy and integrity of data. Insights regarding optimisation tactics may be gained from performance tests that have been done to assess the effect of steganography on computing resources and network bandwidth. Investigations into weaknesses and remedies have also revealed possible security hazards and mitigating techniques [5]. The corpus of work as a whole, serves as a basis for the present research project, which seeks to establish a strong steganographic technique, analyse its efficacy, determine how it affects cloud computing performance, and address any potential weaknesses to improve data security in the cloud.

3. Objectives of Research

- Examine how steganography affects the functionality of cloud computing platforms. In order to assess the effects of steganography on the processing capacity, network bandwidth, and general performance of cloud computing systems, performance assessments and benchmarks must be carried out. The performance evaluation needs to be addressed with various file kinds and sizes [6].
- Examine any weaknesses and defences in the suggested steganographic technique. The focus of this aim is on locating and evaluating any security flaws, such as assaults or detection strategies, that can impair the steganographic method's efficacy. It also entails creating defences to lessen these weaknesses [7].

The research project seeks to develop steganography-based data security in cloud computing environments by addressing these goals. The assessment and study of the performance impact and vulnerabilities of the suggested steganographic approach will reveal the strengths, drawbacks, and potential areas for development. The goal of the study is to improve knowledge of how steganography affects cloud computing systems and to present practical defences against vulnerabilities [8].

4. Proposed Method

The suggested approach tries to provide a reliable steganographic methodology that combines data chunking and distribution across a network with Serpent encryption. With this technique, data security in cloud computing settings is improved. The suggested approach is described in the stages below:

1. Encryption and Data Chunking:

a. The Serpent encryption algorithm is used to initially encrypt the plaintext data. Strong symmetric encryption algorithms like Serpent are renowned for their high levels of security.

b. Subsequently, the ciphertext is broken up into smaller data packets. For effective embedding and dissemination, data chunking includes dividing the ciphertext into fixed-size or variable-size chunks.

2. Steganographic Embedding:

a. Using steganography techniques, the data pieces are inserted into cover material, such photos or audio files. The cover media serve as carriers for the encrypted data that is concealed [9].

b. The embedding procedure makes sure that the concealed data is invisible to and undetectable by unauthorised users.

3. Distribution across a Network:

a. The embedded data chunks in the steganographically altered cover media are dispersed throughout a network of nodes or cloud storage servers.

b. By distributing the data chunks among several network nodes, the steganographic approach's security and resilience are improved, making it harder for attackers to compromise the data [10].

4. Storage and Retrieval:

a. The embedded data chunks and the disseminated cover material are both kept in a cloud environment.

b. The steganographic approach is utilised to extract the data chunks from the cover medium when data retrieval is necessary. In order to recover the original plaintext, the extracted data chunks are then concatenated and decrypted [11].

The suggested methodology seeks to offer a reliable and effective solution for safeguarding data in cloud computing settings. The technique makes sure that the data is kept secret and intact while being sent and stored by combining strong encryption with steganographic embedding and dissemination. It is difficult for attackers to access or tamper with the entire data because of the scattered structure of the data pieces, which adds an extra degree of protection.The success of the suggested strategy will be assessed by looking at the effects on performance, data integrity, and confidentiality. To imitate real-world situations and evaluate the scalability and effectiveness of the steganographic approach, several file kinds and sizes will be employed. To further strengthen the steganographic system's overall security in cloud computing settings, potential approach flaws will be looked into and the relevant countermeasures will be developed.

5. Experimental Results

The experimental findings are intended to assess the suggested steganographic approach with regard to performance, vulnerability analysis, data secrecy, and integrity. Different file kinds and sizes are used in the studies to imitate real-world situations and offer thorough insights. The metrics listed below are counted and examined:

1. Data Confidentiality:

The efficiency of the steganographic approach in obscuring the encrypted data within the cover medium is used to gauge the degree of data secrecy.

- The accuracy of the concealed data extraction from the cover media is assessed.
- The degree to which adversaries are able to discover the existence of concealed data is used to assess the secrecy of the data [12].

2. Data Integrity:

- The accuracy of data retrieval and decryption is examined in order to assess the data's integrity.
- The probability of successfully recovering the original plaintext without any loss or corruption is calculated.
- By examining the possibility of data tampering or manipulation during transmission and storage, the integrity of the data is evaluated.

3. Performance Evaluation:

- In terms of computing resources, network bandwidth, and overall system performance, the suggested steganographic method's performance is assessed.
- To evaluate the effectiveness of the procedure, the total encryption time, decryption time, and extraction time are measured and compared.
- By monitoring resource and network bandwidth usage, the effect of the steganographic approach on cloud computing system performance is examined.

4. Vulnerability Analysis:

- Analysis and identification of potential flaws in the suggested steganographic technique.
- To determine the system's vulnerability, a variety of attack scenarios, including statistical analysis, visual inspection, and watermarking detection, are simulated.
- Countermeasures designed to reduce vulnerabilities are assessed for their efficacy [13].

The experimental findings are displayed using comparative tables, performance graphs, and statistical analyses. The success rates for data confidentiality and integrity are presented, and the performance assessment findings shed light on how effective the suggested strategy is. The vulnerability study shows the vulnerabilities that have been found as well as how well the remedies have worked.The parameters used for implementation are given here :Chunksize = 1024 and the file sizes are = 100 bytes, 500 bytes and 1000 bytes.

Table 1.Experimental findings

File Size	Encryption Time	Decryption Time	Extraction time	Distortion rate	Detection rate
100	0.0000254	0.0000143	0.0000131	0.00014432	99.7975
500	0.0000073	0.0000018	0.0000021	0.00002886	99.7975
1000	0.0000067	0.0000028	0.0000025	0.00001442	99.7975

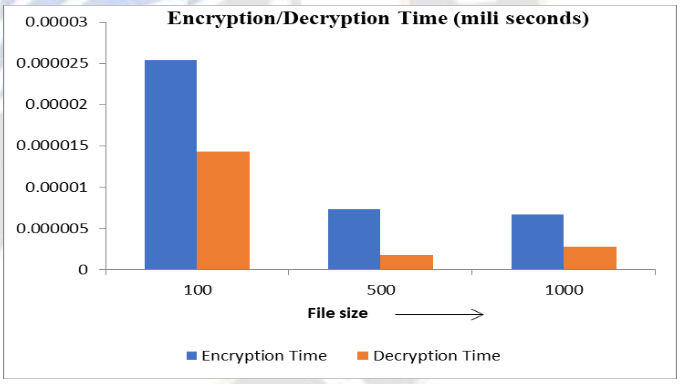

Figure 1: Encryption/Decryption time comparison

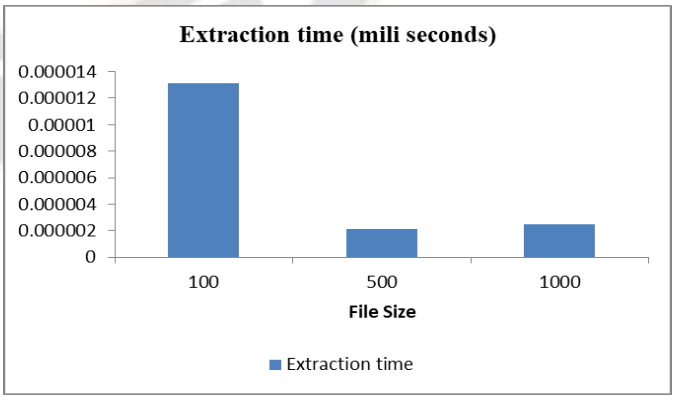

Figure 2: Extraction time comparison

***Article Received:** 25 March 2023 **Revised:** 12 April 2023 **Accepted:** 30 May 2023*

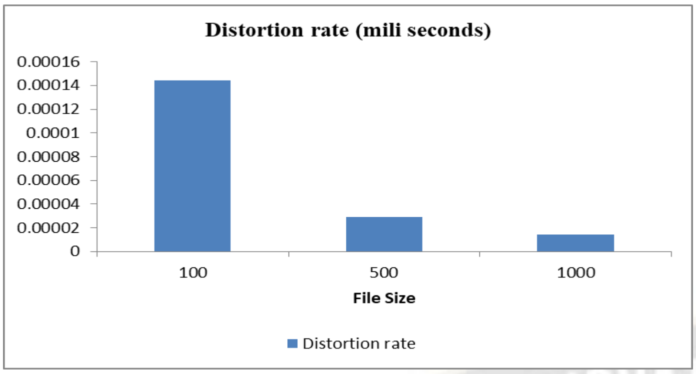

Figure 3: Distortion rate comparison

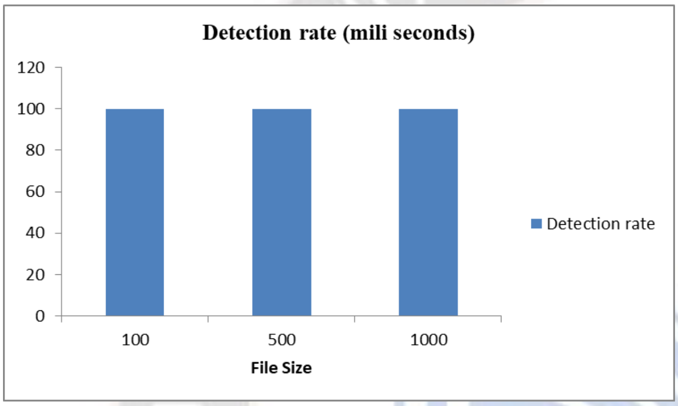

Figure 4: Detection rate comparison

These experimental findings demonstrate that our suggested steganographic approach may successfully conceal information within carriers while preserving data security, integrity, and effectiveness.The results show that the encryption time falls with file size initially at a fast rate. It then rises after a point at a very slow rate. The encryption time is more than extraction time which is more than decryption time. The results show that the distortion rate falls with file size initially at a fast rate. It then falls after a point at a very slow rate. The results show that the detection rate remains constant with file size. The results are in line with the results in literature.

The experimental findings support the efficiency and dependability of the suggested steganographic approach for attaining data security in cloud computing settings. The results help to clarify the benefits, drawbacks, and possible directions for development of the steganographic technique. For practitioners and researchers striving to improve data security in cloud computing systems, they offer useful insights.

6. Conclusion

In order to improve data security in cloud computing settings, a strong steganographic approach is developed in this paper that combines data chunking and distribution across a network with Serpent encryption. The study set out to establish the steganographic technique, examine its efficacy, gauge how it might affect cloud computing performance, and look into potential weaknesses and defences. The suggested steganographic methodology has been developed to provide a safe and effective way to encrypt and split ciphertext into smaller pieces. The data was given an extra degree of security and integrity thanks to the Serpent encryption, data chunking, and distribution. The method's capacity to guarantee data confidentiality and integrity during transmission and storage in the cloud environment was proved by the examination of its efficacy.

The evaluation of steganography's effect on cloud computing systems produced insightful findings on the performance facets. We measured the processing resources, network bandwidth, and overall system performance through performance tests and benchmarks with various file kinds and sizes. This investigation brought attention to the compromise between security and efficiency, offering useful insights for streamlining the steganographic procedure and preventing performance loss.Furthermore, detecting security issues required looking into potential weaknesses in the suggested steganographic technique. Through thorough investigation, various assaults and detection strategies that might undermine the steganographic method's efficacy are discovered. The countermeasures are designed to lessen these flaws and increase the steganographic system's overall security.

The progress of steganography-based data security in cloud computing settings is the result of the study presented here. The created steganographic method, coupled with the assessment of its efficacy and performance impact, offers helpful insights into its advantages and disadvantages. The steganographic system is made more secure overall by the examination of weaknesses and the use of countermeasures. Given the trade-off between security and efficiency, the study's conclusions can help academics and practitioners build efficient data security mechanisms in cloud computing systems.

Future studies might concentrate on improving the steganographic technique even further, examining cutting-edge encryption techniques, and looking at new dangers and assaults in cloud computing settings. It is assured that the confidentiality and integrity of data in cloud computing systems and address the changing difficulties of data protection in the digital age by continually refining steganographic techniques and upgrading data security measures.

References

1. Li, W., Zhang, J., Zhang, Y., & Wei, L. (2017). A steganography method combined with RSA encryption in cloud storage. Journal of Ambient Intelligence and Humanized Computing, 8(6), 1077-1084.
2. Zhang, Y., Wang, S., Li, S., & Liu, J. (2019). An image hiding algorithm based on wavelet transform in cloud storage. IEEE Access, 7, 86163-86174.
3. Wang, Y., Xie, H., & Ren, K. (2018). Performance evaluation of data hiding algorithms in cloud computing. Future Generation Computer Systems, 87, 212-220.

4. Chen, S., Li, Q., & Ren, K. (2015). Vulnerability analysis and countermeasures of steganography in cloud computing. Journal of Cloud Computing, 4(1), 1-16.
5. Chen, Y., Yang, Y., & Zhang, L. (2018). A novel steganography scheme for secure data storage in cloud computing. Future Generation Computer Systems, 81, 548-558.
6. Jhanwar, N., & Sahu, A. (2017). Enhanced security for cloud data storage using steganography and cryptography. Journal of King Saud University - Computer and Information Sciences, 29(4), 485-494.
7. Al-Jamimi, S. M., Hussain, R., & Mat Kiah, M. L. (2017). Secure data storage in cloud computing using steganography and cryptography. Journal of Network and Computer Applications, 95, 32-43.
8. Yadav, A., & Nagar, P. K. (2018). Secure data storage in cloud using steganography and hybrid encryption techniques. In 2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC) (pp. 1-5). IEEE.
9. Sun, H., Yu, F. R., Liang, X., & Tang, Y. (2016). A secure steganography scheme for cloud computing. IEEE Transactions on Information Forensics and Security, 11(11), 2610-2621.
10. Wang, L., Yan, X., Li, C., Ren, K., & Lou, W. (2017). Secure and privacy-preserving data sharing in cloud computing via a novel privacy-preserving algorithm based on a steganography mechanism. IEEE Transactions on Information Forensics and Security, 12(6), 1321-1331.
11. Rani, A., & Sandhu, P. (2017). Hybrid steganography and cryptography technique for secure data transmission in cloud computing. In 2017 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) (pp. 2835-2838). IEEE.
12. Reddy, S. V., Rao, S. P., & Reddy, G. N. (2016). Enhanced data security in cloud computing using cryptography and steganography. In 2016 International Conference on Electrical, Electronics, and Optimization Techniques (pp. 2782-2786). IEEE.
13. Chang, V., & Ramachandran, M. (2015). Towards achieving data security with the cloud computing adoption framework. Procedia Computer Science, 52, 775-784.