Educational Administration: Theory and Practice
2024, 30(6), 1804-1808
ISSN: 2148-2403
https://kuey.net/

Research Article

Secure And Undetectable Multi-Cloud Steganography: Leveraging Non-Alteration Techniques For Covert Communication

Mrs. Salma Banu[1*], Dr. Vijayalaxmi Biradar[2], Dr. Arshad Ahmad Khan Mohammad[3]

[1*]Research Scholar, Kaling University, Email: salmabanuphdece@gmail.com
[2]Associate Professor, Kalinga University
[3]Assistant Professor, Cse -Dept; Gitam University, Email: ibnepathan@gmail.com

***Corresponding Author:** Mrs. Salma Banu
*Research Scholar, Kaling University, Email: salmabanuphdece@gmail.com

Citation: Mrs. Salma Banu et al. (2024), Secure And Undetectable Multi-Cloud Steganography: Leveraging Non-Alteration Techniques For Covert Communication, *Educational Administration: Theory and Practice*, *30*(6), 1804-1808
Doi: 10.53555/kuey.v30i6.5589

ARTICLE INFO

ABSTRACT

Classical steganography faces challenges such as covert channel detection and message loss, while distributed steganography complicates detection through cloud storage by fragmenting messages across varied media. A novel multi-cloud steganography paradigm addresses these issues by distributing secrets without altering files, bolstering security and undetectability. This approach seamlessly integrates information using a covert channel model, strategically arranging clouds, authenticating accounts, and utilizing disjointed file lists. A critical examination of the method's security strength challenges claims of computational infeasibility, suggesting enhancements for increased security against brute force attacks. The accompanying paper underscores the dynamic nature of steganography in multi-cloud environments, emphasizing the continuous need for robust security measures in this intricate field.

Keywords: Steganography, Multi-cloud environments, Security, Undetectability, Brute-force attacks

1. Introduction

Classical steganography hides the secret data within various types of cover media, aiming to make secret data undetectable to unauthorized users [4]. However, it faces challenges like covert channel detection, being detected by attackers, and risk of losing the secret data due to modifications. In response, distributed steganography fragments secret data across diverse cover media, further utilizes cloud technologies for extra layer of protection [4]. Despite its advantages, vulnerabilities may arise due to the need to modify media, posing a security risk. Both mechanisms aim is to store secret securely, but distributed steganography offers extended security by dispersing data across multiple locations. To address the problem, a new steganography concept developed by two technical objectives I). cover media does not undergo any modification, i.e., the cover media act as a pointer to fragmented data II). A secret message is stored in the multi-cloud storage environment [1,2,3]. It claims that it is computationally infeasible for an attacker to detect and extract the hidden message despite of having fully access to the accounts of the different clouds. This approach relies on a covert channel model, seamlessly integrating information into files without observable changes. Our motivation is to build upon this foundation, enhancing security and undetectability in secret storage and retrieval.
Another work [2] critically examines the security strength of the approach [4], challenging claims of computational infeasibility against brute force attacks. Work analysed the security strength of the novel steganography concept and concluded that, attacker can get the secret value stored in multi-cloud storage environment using the brute force attacks more diminutive than exponential computations. This scrutiny underscores the need for stronger security measures in this steganography approach. Our motivation lies in addressing potential vulnerabilities and advancing the field to ensure secure and efficient secret storage and retrieval. This paper introduces a novel steganography method for secure data concealment in multi-cloud environments, utilizing unchanged cover media as references for fragmented data across multiple clouds. This

innovative approach avoids file modifications and increases resistance against brute-force attacks, contributing to secure secret storage and retrieval.
The aim of this paper is to introduce and evaluate a novel steganography method for secure data concealment in multi-cloud environments. Our objective is to address the limitations of existing steganography techniques, particularly in terms of security vulnerabilities and detectability, by leveraging unchanged cover media as references for fragmented data across multiple clouds. Specifically, we aim to:

1. Develop a steganography approach that does not require modifications to cover media, enhancing security and reducing the risk of detection.
2. Utilize multi-cloud storage environments to disperse secret data, increasing resistance against brute-force attacks and unauthorized access.
3. Evaluate the computational feasibility and security strength of the proposed method, comparing it to existing techniques and addressing potential vulnerabilities.

The core objective of our proposed work is to contribute to the ongoing evolution of secure communication in multi-cloud environments by introducing an innovative embedding algorithm for the strategic distribution of secrets across cloud platforms. Utilizing file lists within clouds as a hiding medium ensures heightened security and resistance to steganalysis. We aim to demonstrate the effectiveness of this system in enhancing security and undetectability in secret storage and retrieval within complex multi-cloud environments. Beyond presenting a novel approach, our research critically analyzes the proposed scheme's security strength, addressing potential vulnerabilities, and proposing enhancements for robust security against various attacks. This motivation underscores the significance of continually advancing steganography methods for secure secret storage and retrieval in the ever-evolving landscape of multi-cloud environments.

2. Proposed work

In the pursuit of advancing secure communication within multi-cloud environments, this proposed work introduces the Non-Alteration Multi-Cloud Steganography scheme. The escalating demand for secure data concealment and retrieval necessitates innovative solutions that address the shortcomings of classical and distributed steganography. The core objective is to establish a robust and undetectable method for distributing secrets across multiple clouds without altering the original files, thereby enhancing the security and confidentiality of covert communication.
Traditional steganography faces challenges related to covert channel detection, potential discovery by attackers, and risks associated with alterations or deletions in cover media. Distributed steganography, while an evolution, still involves modifying media, posing a potential risk to message security. The proposed work aims to overcome these challenges by introducing a scheme that strategically distributes secrets without altering original files, thereby minimizing detection risks and ensuring secure data concealment in multi-cloud environments.
Motivated by the imperative need for secure communication in the intricate landscape of multi-cloud environments, the Non-Alteration Multi-Cloud Steganography scheme is conceived. The motivation stems from the inadequacies of existing steganography methods, which either compromise security by altering files or risk detection due to suspicious modifications. This work aspires to provide a secure, undetectable, and non-intrusive means of covert communication, fostering confidentiality and integrity in the transmission of sensitive information.
The primary objective is to introduce a novel steganography scheme tailored for multi-cloud environments, ensuring secure data embedding without altering original files. The proposed Non-Alteration Multi-Cloud Steganography seeks to establish a new standard for covert communication by strategically distributing secrets, enhancing security against brute-force attacks, and making secret data retrieval computationally infeasible for attackers. The scheme aims to contribute to the advancement of secure communication paradigms within the complex and dynamic realm of multi-cloud environments
Non-Alteration Multi-Cloud Steganography The proposed algorithm delineates the intricate steps for both embedding and extracting secret information within a multi-cloud environment. Consider an implementation scenario where Alice and Bob decide to securely store and retrieve a numerical secret in a multi-cloud environment using the Non-Alteration Multi-Cloud Steganography scheme.
The proposed steganography algorithm comprises several intricately designed steps, each playing a crucial role in ensuring the security and controlled distribution of the original secret within a multi-cloud environment. Initiated by the encryption of the transcoded secret using the Advanced Encryption Standard (AES) and a shared secret key, the algorithm produces a 128-bit ciphertext. This ciphertext is then subjected to secret transcoding and block formation, breaking it into manageable 8-bit blocks and converting them into decimal numbers, forming a matrix S that represents the encrypted secret. The subsequent step involves the generation of a randomization parameter (R) through a secure shuffling algorithm applied to matrix S, followed by the application of the XOR operation between S and R. This introduces an element of unpredictability and complexity. The double-columnar transposition, facilitated by a shared key, rearranges the XOR results, yielding a list E of 4-bit binary blocks. These blocks are then substituted into clouds, each associated with a distinct subset of files from predefined lists (L1, L2, L3, L4). The careful mapping ensures that each bit in a

cloud corresponds to a specific file in the respective list, achieving a secure and controlled distribution of the original secret. The cloud representation elucidates how each cloud holds a binary sequence representing a subset of files, showcasing the algorithm's efficacy in secure information distribution. In essence, this comprehensive algorithm combines encryption, transcoding, randomization, transposition, and substitution to create a robust and effective steganography scheme tailored for multi-cloud environments. The following example provides a step-by-step illustration:

Initial Agreements:

1. **Shared Key Information and Encryption Details:**

1. Number of Clouds (n)
2. Lists ($L^0, L^1, L^2, L^3 \dots \dots$)
3. Base Value (B)
4. Encryption Algorithm: AES
5. Encryption Mode: CBC
6. Shared Key (K): [Shared Secret Key]

Embedding Process

Step 1: Encryption of the Secret

1. **Input:** Transcoded secret **s**, Shared Secret Key **K**.
2. Employ Advanced Encryption Standard (AES) to encrypt **s** with the secret key **K**.
3. Obtain a 128-bit ciphertext **C**.

Step 2: Secret Transcoding and Block Formation

1. **Input:** Ciphertext **C**.
2. Partition **C** into 8-bit blocks.
3. Convert each 8-bit binary block into decimal numbers.
4. Form a matrix **S** with decimal values, representing the secret.

Step 3: Randomization Parameter (R) Generation

1. Generate a randomization parameter **R** by applying a secure shuffling algorithm to matrix **S**.
2. Apply the XOR operation between matrix **S** and **R**.

- For each block in **S**, use the Fisher-Yates shuffling algorithm.

Step 4: Double-Columnar Transposition

1. **Input:** XOR results.
2. Apply a double-columnar transposition using a shared key.
3. Result in a list **E** of 4-bit binary blocks.

Step 5: Substitute Cloud Values with Respective List Files

1. **Input:** List **E**, Lists **L1**, **L2**, **L3**, **L4**.
2. Substitute binary values in **E** with corresponding files from lists **L1**, **L2**, **L3**, **L4**.
3. Each bit in a cloud corresponds to a file in the respective list, achieving secure information distribution.

Cloud Representation:

- C0 Cloud:
- A binary sequence representing a subset of files from **L1**.
- C1 Cloud:
- A binary sequence representing a subset of files from **L2**.
- C2 Cloud:
- A binary sequence representing a subset of files from **L3**.
- C3 Cloud:
- A binary sequence representing a subset of files from **L4**.

This algorithm ensures the confidentiality of information through AES encryption, transcoding, and secure shuffling. Double-columnar transposition and cloud substitution further enhance security and enable secure distribution of information across distinct clouds. The approach is designed to be effective and applicable in a variety of contexts where secure information sharing is critical.

Extraction Process

1. **Input:**

- **result_clouds**: Clouds obtained after embedding.
- **shared_key**: Cryptographic key shared between communicating parties.

2. **Step 1: File Extraction and Cloud Reconstruction**

- Extract files from each cloud in **result_clouds**.
- Reverse the process of file substitution and cloud formation.

3. **Step 2: Cloud-to-Bit Decoding**

- Decode bits from each cloud to obtain the original 4-bit binary blocks.

4. Step 3: Reverse Columnar Transposition

- Reverse the double-columnar transposition using the **shared_key**.
- Output: Matrix **S** of decimal numbers.

5. Step 4: Reverse Randomization Parameter Application

- Reverse the XOR operation between **S** and **R** to obtain the original matrix **S**.

6. Step 5: Reverse AES Decryption

- Reverse the AES encryption using the **shared_key** to obtain the original **secret**.

7. Output:

- Display the extracted **secret** with utmost confidentiality.

3. Performance Analysis of Non-Alteration Multi-Cloud Steganography

1. Base Value Impact:

- The chosen base value (**B**) significantly influences the capacity and efficiency of the secret distribution process.
- Smaller bases result in a higher number of distributed values, but larger bases reduce the number of lists needed.

2. File Lists and Base Value Relationship:

- The base value directly correlates with the number and size of file lists required for secret dissimulation.
- Each list's size aligns with the chosen base, optimizing the embedding process.

3. File Extension Versatility:

- The scheme exhibits remarkable versatility, supporting various file extensions for covert communication.
- Integration with word, excel, PowerPoint, and PDF files maintains file integrity, expanding application scenarios.

4. Multi-Cloud Environment:

- The utilization of multiple cloud accounts from different providers (SugarSync, Dropbox, OneDrive, Google Drive) demonstrates scalability and diversification.
- The multi-cloud approach enhances security by distributing secret segments across diverse platforms.

5. Optimal Secret Distribution:

- Example 4 illustrates the scheme's capability for optimal secret distribution, minimizing files deposited in each cloud.
- This optimization streamlines secret extraction, reducing search time for files within lists.

6. Security Strength:

- The scheme demonstrates strength against traditional steganalysis techniques due to its non-alteration approach.
- The absence of modifications in cover media enhances covert communication undetectability.

7. Adversarial Hypothesis 1: No Cloud Access:

- The scheme proves robust against adversaries lacking cloud access and unaware of key, file lists, and base values.
- Covert communication remains undetected, with no suspicious additions in exchanged files.

8. Adversarial Hypothesis 2: Partial/Full Cloud Access:

- Adversaries with partial/full cloud access face insurmountable challenges due to the exponential permutations required for a successful attack.
- Lack of direct communication between parties and the covert channel's cloud-centric nature disrupts traditional security models.

9. File Integrity Preservation:

- The scheme ensures file integrity preservation by relying on file lists within clouds, avoiding modifications to original files.
- This feature contributes to the robustness of the scheme against potential attacks.

10. Comparison with Existing Work:

- Our approach, unlike conventional techniques, distributes secrets without altering original files, providing heightened security.
- The embedding algorithm strategically distributes secrets, while the extraction algorithm ensures secure retrieval.

11. Advancements and Future Directions:

- The proposed system represents a significant advancement in steganography within multi-cloud environments.
- Future research aims to optimize parameters for enhanced secret distribution and assess the scheme's robustness with very large secret data.

4. Conclusion

The Non-Alteration Multi-Cloud Steganography scheme offers a promising solution to challenges in distributed environments. Its effective performance, robust security features, and file integrity preservation make it a noteworthy advancement in the field. The scheme's ability to conceal secrets without altering original files, combined with its resilience against steganalysis, positions it as a secure and practical option for covert communication in intricate multi-cloud landscapes.

References

1. Arif, Mohammad Abdul, et al. "Brute Force Attack on Distributed data Hiding in the Multi-Cloud Storage Environment More Diminutive than the Exponential Computations." *Ingenierie des Systemes d'Information* 27.6 (2022): 915.
2. Hashmi, S.S., Mohammad, A.A.K., Abdul, A.M., Atheeq, C., Nizamuddin, M.K. (2024). Enhancing data security in multi-cloud environments: A Product Cipher-Based Distributed Steganography approach. International Journal of Safety and Security Engineering, Vol. 14, No. 1, pp. 47-61. https://doi.org/10.18280/ijsse.140105
3. Abdul, Arif Mohammad, et al. "Enhancing Security of Mobile Cloud Computing by Trust-and Role-Based Access Control." *Scientific Programming* 2022 (2022).
4. Moyou Metcheka, Leonel, and René Ndoundam. "Distributed data hiding in multi-cloud storage environment." *Journal of Cloud Computing* 9.1 (2020): 68.
5. Ijteba Sultana, Dr. Mohd Abdul Bari ,Dr. Sanjay," Routing Performance Analysis of Infrastructure-less Wireless Networks with Intermediate Bottleneck Nodes", International Journal of Intelligent Systems and Applications in Engineering, ISSN no: 2147-6799 IJISAE,Vol 12 issue 3, 2024, Nov 2023
6. Dr. Mohammed Abdul Bari,Arul Raj Natraj Rajgopal, Dr.P. Swetha ," Analysing AWSDevOps CI/CD Serverless Pipeline Lambda Function's Throughput in Relation to Other Solution", International Journal of Intelligent Systems and Applications in Engineering , JISAE, ISSN:2147-6799, Nov 2023
7. Abdul Rafey, Mohammed Sufiyan Ali Quadri, Ali Bin Abdullah Nahd, Dr. Mohammed Abdul Bari ," Pothole Detection Technique", Mathematical Statistician and Engineering Applications, ISSN: 2094-0343, 2326-9865, Vol 72 No. 1 (2023), Page Number: 1316-1327
8. Mohammed Osman Uddin Jaber Mohammed Faizan Mohammed Riyaaz Dr. Mohd Abdul Bari," Virtual College Receptionist Based On Android", Journal of Information and Computational Science , ISSN: 1548-7741, Volume 11 Issue 5 – 2021