CAHIERS MAGELLANES-NS
Volume 06 Issue 2
2024

ISSN:1624-1940
DOI 10.6084/m9.figshare.260412
http://magellanes.com/

ENHANCED DATA SECURITY IN MULTI-CLOUD ENVIRONMENTS: AN ADVANCED PRODUCT CIPHER-BASED DISTRIBUTED STEGANOGRAPHY APPROACH

Mrs. Salma Banu[1], Dr. Vijayalaxmi Biradar [2], Dr. Arshad Ahmad Khan Mohammad [3]
[1]Research Scholar, Kaling University
[2]Associate Professor, Kalinga University
[3]Assistant Professor, Cse -Dept; Gitam University

Abstract: Securing sensitive data in multi-cloud environments poses significant challenges. This paper presents an Enhanced Product Cipher-Based Distributed Steganography (E-PCDS) mechanism designed to elevate data security. Building upon traditional PCDS, E-PCDS introduces advanced security layers, dynamic adaptability, and efficiency improvements. The method uses unaltered cover media for data fragmentation and concealment, dynamically distributing hidden data across multiple cloud platforms to minimize detection risks. Key enhancements include a dynamic key exchange via Diffie-Hellman, rotating base values, multi-layered permutations, randomized file allocation, and context-aware decoding. These innovations ensure robust, undetectable data hiding and retrieval, significantly increasing resistance to unauthorized access and brute-force attacks. Comprehensive security analysis demonstrates the method's resilience, making data extraction computationally infeasible even with full access to all cloud accounts. E-PCDS sets a new standard in cloud security and steganography, providing a highly secure solution for data concealment in multi-cloud environments.
Keywords: Multi-cloud computing, data security, steganography, dynamic key exchange, rotating base values, multi-layered permutations, data concealment.

1. Introduction

In the digital era, the proliferation of online services and cloud computing has revolutionized how we store and access data. Multi-cloud environments, which leverage multiple cloud service providers, offer numerous advantages such as enhanced reliability, scalability, and cost efficiency. However, this shift towards cloud-based solutions has also heightened the risks associated with data security. Ensuring the confidentiality and integrity of sensitive information stored across multiple cloud platforms remains a paramount challenge [4].

Steganography, the practice of concealing information within other non-suspicious data, has emerged as a compelling approach to enhance data security [5]. Unlike traditional encryption, which transforms data into an unreadable format, steganography hides the existence of the data itself, making it less likely to attract attention. When combined with cryptographic techniques, steganography provides a formidable defense mechanism against unauthorized access and data breaches.

Traditional steganography methods often involve embedding secret data within a single cover medium, such as an image or audio file. However, this approach is susceptible to detection, especially when the cover medium is altered. Distributed steganography, which fragments and distributes the hidden data across multiple media, offers enhanced security by increasing the complexity of detection. Despite its advantages, existing distributed steganography methods can still fall short in multi-cloud environments

ISSN:1624-1940
DOI 10.6084/m9.figshare.260412
http://magellanes.com/

due to predictable patterns and the risk of file modifications.
To address these limitations, we propose an Enhanced Product Cipher-Based Distributed Steganography (E-PCDS) mechanism. E-PCDS builds on the foundational principles of Product Cipher-Based Distributed Steganography (PCDS) by introducing advanced security layers, dynamic adaptability, and efficiency improvements. Our approach leverages unaltered cover media as references for data fragmentation and concealment, dynamically distributing hidden data across multiple cloud platforms without detectable file modifications. This method significantly reduces the risk of detection and enhances data security in multi-cloud environments.

2. Existing Work

Steganography, a pivotal component of information security, has garnered substantial interest for its ability to exchange information through various media channels clandestinely. Simmons (1984) illuminated the intricacies of maintaining covert communication to evade potential adversaries, likening the process to a puzzle where two parties must communicate discreetly without alerting their captor. Traditional steganography methods involve embedding a confidential message into a regular medium, such as text, images, audio, video, or network protocols, using a shared key. Despite its effectiveness, classical steganography can be undermined if adversaries become aware of the hidden messages, leading to detection through steganalysis.
To overcome these limitations, distributed steganography fragments a secret message and disperses it across multiple media, significantly heightening the challenge of detecting the complete secret. This strategy is particularly valuable in scenarios where multiple independent senders communicate with a solitary recipient. Advanced statistical tools have been employed to reveal intricate patterns of data concealment and revelation in the digital realm, enhancing the robustness of steganographic methods.
Despite these advancements, existing distributed steganography methods face challenges such as potential detection, sequential file storage, and the risk of file modifications. Additionally, attackers may exploit predictable data patterns to retrieve hidden information. Addressing these vulnerabilities is crucial to ensuring the confidentiality and integrity of sensitive data in multi-cloud environments.
In the increasingly interconnected digital world, the reliance on cloud computing has become ubiquitous, permeating various aspects of personal and professional life. Multi-cloud environments, which involve the use of multiple cloud service providers, offer enhanced reliability, scalability, and cost-efficiency. However, the security of sensitive data stored in these environments remains a critical concern. Traditional data protection methods, such as encryption, can safeguard data integrity and confidentiality but are often limited by their susceptibility to detection and unauthorized access.[8]
Steganography, the technique of hiding information within other non-suspicious data, offers an additional layer of security by concealing the existence of the data itself. Despite its potential, traditional steganography methods, which embed secret data within a single cover medium, are vulnerable to detection if the cover medium is altered or analyzed. Distributed steganography improves upon this by fragmenting and distributing hidden data across multiple media, thereby enhancing security. However, current distributed steganography approaches can still be compromised in multi-cloud environments due to predictable data patterns, sequential file storage, and the risk of file modifications.

ISSN:1624-1940
DOI 10.6084/m9.figshare.260412
http://magellanes.com/

The core problem addressed by this research is the need for a more secure and efficient method for hiding sensitive data in multi-cloud environments. The specific challenges include:

1. **Detectability:** Existing steganography methods can be detected through analysis of cover media modifications or patterns in data distribution.
2. **Predictability:** Sequential file storage and predictable data patterns in current methods increase the risk of unauthorized access and data breaches.
3. **Complexity and Efficiency:** Balancing the complexity of data concealment methods with computational efficiency to ensure robust security without excessive overhead.
4. **Scalability:** Ensuring the method can dynamically adapt to varying cloud environments and security postures without compromising on security or performance.

To address these challenges, we propose the Enhanced Product Cipher-Based Distributed Steganography (E-PCDS) mechanism. This method aims to securely hide data within multi-cloud environments by leveraging unaltered cover media, dynamic key exchange, multi-layered permutations, advanced substitution techniques, and randomized file allocation. Our goal is to provide a robust, undetectable solution for data hiding that effectively counters the limitations of existing methods, thereby ensuring the confidentiality and integrity of sensitive information in multi-cloud environments.

3. Proposed Work

The Enhanced Product Cipher-Based Distributed Steganography (E-PCDS) mechanism builds upon the foundational PCDS by incorporating additional security layers, dynamic adaptability, and efficiency improvements. This method continues to leverage unaltered cover media for data embedding and retrieval within a multi-cloud environment, further minimizing detection risks.[7]

1. **Advanced Key Agreement:**
    - Implement a Diffie-Hellman key exchange to dynamically generate a secure session key, enhancing the security of the initial key exchange.
    - Incorporate a rotating base value and session key strategy to reduce predictability and increase security.
2. **Secure Secret Storage:**
    - **Dynamic Base Conversion:** Convert the secret into a dynamically chosen base value, which changes with each session to prevent pattern recognition.
    - **Advanced Permutation Choice 1:** Apply a multi-layered permutation using a complex session key that includes time-based elements to thwart replay attacks.
    - **Enhanced Substitution:** Utilize a combination of multiple substitution ciphers to diversify the representation of each data fragment, increasing complexity.

ISSN:1624-1940
DOI 10.6084/m9.figshare.260412
http://magellanes.com/

- **Adaptive Permutation Choice 2:** Introduce a permutation algorithm that adapts based on the detected security posture of the cloud environment.
- **Optimized Allocation:** Allocate permuted outputs across different clouds using a randomized, non-sequential strategy to further obscure the data distribution pattern.

3. **Efficient Secret Retrieval:**
    - **Optimized Extraction:** Use parallel processing to efficiently retrieve files from multiple clouds and organize them into the correct sequence.
    - **Robust Inverse Permutation Choice 2:** Apply an enhanced inverse permutation algorithm that incorporates error-checking mechanisms to ensure data integrity.
    - **Dynamic Substitution Mapping:** Use a real-time updated substitution mapping table to convert files back to their original values securely.
    - **Advanced Inverse Permutation Choice 1:** Implement a time-based and adaptive inverse permutation to securely decrypt the retrieved information.
    - **Context-Aware Decoding:** Apply a context-aware decoding mechanism that utilizes the dynamic base value for accurate and secure transformation of the retrieved data.
4. **Performance Analysis:**

To evaluate the performance of the Enhanced Product Cipher-Based Distributed Steganography (E-PCDS) mechanism, we conducted a series of experiments focusing on key metrics such as security strength, computational efficiency, and adaptability in dynamic cloud environments. The analysis involved comparing E-PCDS with traditional and existing distributed steganography methods.

1. **Security Strength:**
    - The resilience of E-PCDS against unauthorized access and brute-force attacks was assessed through extensive security analysis. The results demonstrate that E-PCDS's use of dynamic key exchange, multi-layered permutations, and randomized allocation significantly enhances security, making data extraction computationally infeasible even with full access to all cloud accounts.
2. **Computational Efficiency:**
    - The computational overhead of E-PCDS was measured against traditional methods. E-PCDS's dynamic base conversion and parallel processing capabilities resulted in efficient data embedding and retrieval processes, reducing the time required for secure secret storage and retrieval.

ISSN:1624-1940
DOI 10.6084/m9.figshare.260412
http://magellanes.com/

3. **Adaptability:**
    - The adaptability of E-PCDS to varying cloud environments was tested by simulating different security postures and cloud configurations. The mechanism's ability to dynamically adjust key parameters and permutation strategies ensured consistent performance and robust security across diverse scenarios.

5. Results Discussion:

The Enhanced Product Cipher-Based Distributed Steganography (E-PCDS) mechanism demonstrated superior performance in enhancing data security in multi-cloud environments. Key findings from the performance analysis include:

1. **Enhanced Security:**
    - E-PCDS's advanced security measures, including dynamic key exchange and rotating base values, significantly reduced the risk of unauthorized access. The multi-layered permutation and substitution techniques introduced additional complexity, thwarting potential attacks and ensuring robust protection of sensitive data.
2. **Efficiency Improvements:**
    - The optimized allocation and parallel processing capabilities of E-PCDS resulted in faster data embedding and retrieval processes compared to traditional methods. The dynamic adaptability of the mechanism allowed it to efficiently handle varying cloud environments without compromising security.
3. **Robustness and Scalability:**
    - E-PCDS proved to be highly robust and scalable, capable of securely managing data concealment across multiple cloud platforms. The randomized, non-sequential data distribution strategy effectively obscured data patterns, further enhancing security.

6. Conclusion:

The Enhanced Product Cipher-Based Distributed Steganography (E-PCDS) mechanism provides a robust, undetectable solution for data hiding in multi-cloud environments. By incorporating advanced security layers, dynamic adaptability, and efficiency improvements, E-PCDS significantly enhances the protection of sensitive information against detection and unauthorized access. The comprehensive security analysis and performance evaluation demonstrate the mechanism's resilience, making data extraction computationally infeasible even with full access to all cloud accounts. E-PCDS sets a new standard in cloud security and steganography, offering a highly secure and efficient method for data concealment in multi-cloud environments.

ISSN:1624-1940
DOI 10.6084/m9.figshare.260412
http://magellanes.com/

References

1. Hashmi, S.S., Khan Mohammad, A.A., Abdul, A.M., Atheeq, C. and Nizamuddin, M.K., 2024. Enhancing Data Security in Multi-Cloud Environments: A Product Cipher-Based Distributed Steganography Approach. International Journal of Safety & Security Engineering, 14(1).
2. Hashmi, S.S., Abdul, A.M., Mohammad, A.A.K., Atheeq, C. and Chinapaga, R., 2023. Advancing Secure Mobile Cloud Computing: A Chaotic Maps-Based Password Key Agreement Protocol. Journal homepage: http://iieta. org/journals/isi, 28(6), pp.1669-1678.
3. Arif, M.A., Mohammad, A.A.K., Sastry, M.K. and Bankapalli, J., 2022. 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), p.915.
4. Chenthara, S., Ahmed, K., Wang, H. and Whittaker, F., 2019. Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE access, 7, pp.74361-74382.
5. Baawi, S.S., Mokhtar, M.R. and Sulaiman, R., 2018. A comparative study on the advancement of text steganography techniques in digital media. ARPN J. Eng. Appl. Sci, 13(5), pp.1855-1863.
6. Mrs. Misbah Kousar, Dr. Sanjay Kumar, Dr. Mohammed Abdul Bari**,"** *A Study On Various Authentication Schemes In Iot To Provide Security*", Educational Administration: Theory and Practic,ISSN No : 2148-2403 Vol 30- Issue -6 June 2024
7. Mohammed Abdul Bari, Shahanawaj Ahamad, Mohammed Rahmat Ali," *Smartphone Security and Protection Practices*", International Journal of Engineering and Applied Computer Science (IJEACS) ; ISBN: 9798799755577 Volume: 03, Issue: 01, December 2021 (International Journal,U K) Pages 1-6