IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 11, Issue 6, November-December 2024

Impact Factor: 7.394

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106056

Data Integrity Audit Based on Data Blinding for Cloud and Fog Environment

R.Rajesh Goud, P.Dilip, Varun Teja, P.Sunil

Student, Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India

Student, Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India

Student, Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India

Assistant Professor, Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India

ABSTRACT: Traditional data integrity auditing in cloud and fog environments often struggles with challenges like low data security, slow processing speeds, and inefficient communication. This paper introduces a novel data integrity audit scheme based on data blinding to address these issues. Our proposed scheme leverages edge devices to form a fog computing layer between the cloud service provider and the data owner, effectively reducing transmission delays. A blind factor is introduced during the integrity audit process to prevent data leakage and unauthorized access. The proposed system architecture includes three entities: the data owner, the fog node, and the cloud server. By implementing a blind signature protocol, the scheme enhances data security during transfer and storage. The security model and proof are based on computational Diffie-Hellman (CDH) assumptions, ensuring robust security guarantees. Extensive experimental results demonstrate that the integration of the fog computing layer and data blinding technique not only significantly reduces data communication delays but also improves the security and efficiency of the data integrity audit process. This approach ensures that data remains secure and intact, addressing both practical and theoretical aspects of data integrity in modern computing environments.

I. INTRODUCTION

In recent years, the growing abundance of information has increased the storage and computing demands on various terminal devices like mobile phones and computers. To alleviate this burden, many users store their data in the cloud. However, cloud service providers may sometimes delete infrequently used data to reduce server overhead, leading to potential data loss. This situation has made remotely checking the integrity of uploaded data an urgent issue.

The concept of Remote Data Possession Checking (RDPC), which includes proof of retrievability (POR) and provable data procession (PDP), has been proposed to address these challenges. RDPC can be categorized into private and public audits. Private audits are conducted by the data owner, while public audits can be performed by any authorized thirdparty auditor, with public auditing being more flexible and commonly used.

As cloud computing becomes increasingly popular, more users are storing their data in the cloud for easy access. However, the traditional cloud storage model requires each user to establish a connection with the cloud service provider, increasing the provider's load pressure. Additionally, long-distance data transmission can occupy bandwidth and cause delays.

To mitigate these issues, the concept of fog computing has been introduced. Fog computing, which is closer to the data owner than traditional cloud computing, adds a fog node layer to reduce transmission delays and bandwidth usage. However, existing schemes, such as those proposed by Hu et al. and Yan et al., have limitations regarding security and privacy protection in the fog computing framework, leading to potential information leakage.

II. EXISTING SYSTEM

In the realm of supply chain networks, most current tracking and traceability systems are plagued by significant issues due to their reliance on centralized management. This centralized approach often leads to serious data privacy concerns, as the central authority has access to all data, making it a prime target for cyber-attacks. Additionally, centralized systems can suffer from single points of failure, which can disrupt the entire network if the central server experiences issues.

Traditional data integrity auditing methods also face several challenges. These include low data security, as these methods might not provide robust protection against unauthorized access or tampering. Additionally, they tend to have slow data processing speeds, which can hinder realtime applications and lead to inefficiencies in data handling. Communication efficiency is another major problem, as the existing systems often have high latency and bandwidth usage, which can slow down the entire process and affect the overall performance of the network.

Furthermore, the current technology, which is predominantly based on symmetric key encryption, does offer some level of security. It supports various operations such as block modification, deletion, and append, making it flexible to some extent. However, this technology has its limitations and does not adequately address the broader challenges of ensuring high data security, speed, and efficient communication within the network.

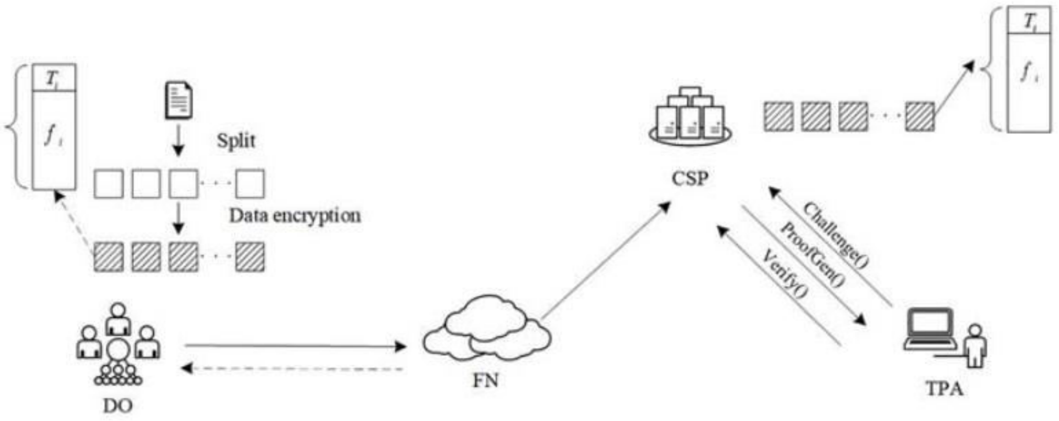
Overall, the existing systems and technologies exhibit several shortcomings that need to be addressed to improve the efficiency, security, and reliability of data integrity auditing and supply chain tracking.

III. PROPOSED SYSTEM

This paper introduces a new data integrity audit scheme based on the cloud and fog architecture, utilizing computational Diffie-Hellman (CDH) assumptions to provide a robust security model and proof. The proposed system includes a data transmission model within the cloud and fog network, where data is transmitted and processed by fog nodes to identify the optimal communication channels, thereby reducing communication overhead.

To enhance security, a blind factor is incorporated during the evidence generation stage of the integrity audit. This prevents adversaries from calculating ciphertexts during multiple interrogations, significantly improving the security of the audit process. Additionally, the paper explores a new service mechanism designed to optimize profits for both the cloud provider and its multiple users. By adopting a game-theoretic approach, the relationship between the cloud provider and its users is modeled as a Stackelberg game, where user strategies depend on the cloud provider's actions.
In this mechanism, the cloud provider aims to select appropriate servers and configure an effective request allocation strategy to minimize energy costs while ensuring user satisfaction. This approach aims to balance the provider's resource management with the users' needs, offering an efficient and secure solution for data integrity audits in cloud and fog environments

System Architecture:



System Architecture Model

Software Testing
General: Testing aims to discover errors in software products by checking the functionality of components, sub-assemblies, and finished products. It ensures that the software meets requirements and user expectations.

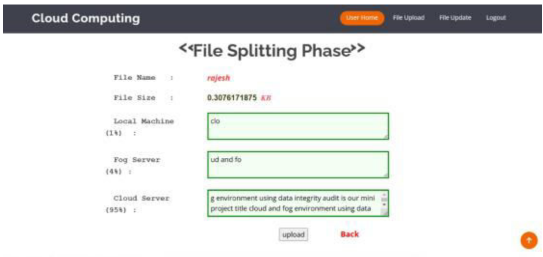
Developing Methodologies: The test process starts with a comprehensive plan to test general functionality and special features across various platforms. Strict quality control procedures ensure that the application meets the specified requirements and is bug-free.

Types of Tests: Unit Testing: Validates internal program logic and outputs at the component level.

- Functional Testing: Demonstrates that functions work as specified by business and technical requirements.
- System Testing: Ensures the entire integrated system meets requirements and produces predictable results.
- Performance Testing: Verifies that output is produced within time limits and system response times are acceptable.
- Integration Testing: Checks for errors in interactions between integrated software components.
- Acceptance Testing: Ensures the system meets functional requirements, involving significant end-user participation.

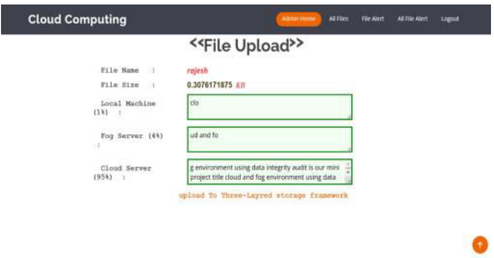
Test Cases: Include positive and negative test cases to validate expected and unexpected outcomes.
Test Plan: Divides the project into units, performs detailed processing, and identifies bugs for correction.
Applications and Future Enhancement
General: Public auditing offers higher flexibility and is commonly chosen. Fog computing, closer to the data owner, reduces transmission delay and bandwidth usage.
Future Enhancement: Performance analysis shows the protocol is efficient. Future work will improve the fog computing layer's architecture for better efficiency.
Conclusion
The paper proposes a DBCF protocol for data security in cloud and fog environments, introducing a blind factor in data verification to prevent adversary access. The fog computing layer reduces communication overhead, and the protocol is proven secure under the CDH assumption.

IV. RESULTS



<<File Splitting Phase>>

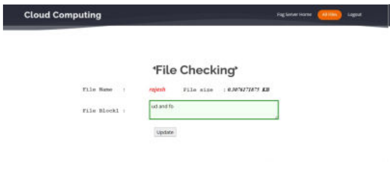
File Name : rajesh
File Size : 0.3076171875 KB
Local Machine (1%) : clo
Fog Server (4%) : ud and fo
Cloud Server (95%) : g environment using data integrity audit is our mini project title cloud and fog environment using data



<<File Upload>>

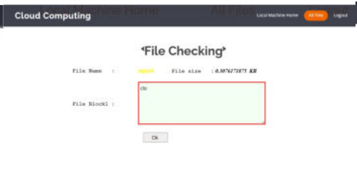
File Name : rajesh
File Size : 0.3076171875 KB
Local Machine (1%) : clo
Fog Server (4%) : ud and fo
Cloud Server (95%) : g environment using data integrity audit is our mini project title cloud and fog environment using data

upload To Three-Layred storage framework



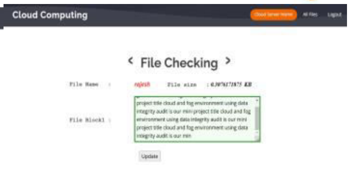
File Checking

File Name : rajesh File size : 0.3076171875 KB
File Block1 : ud and fo



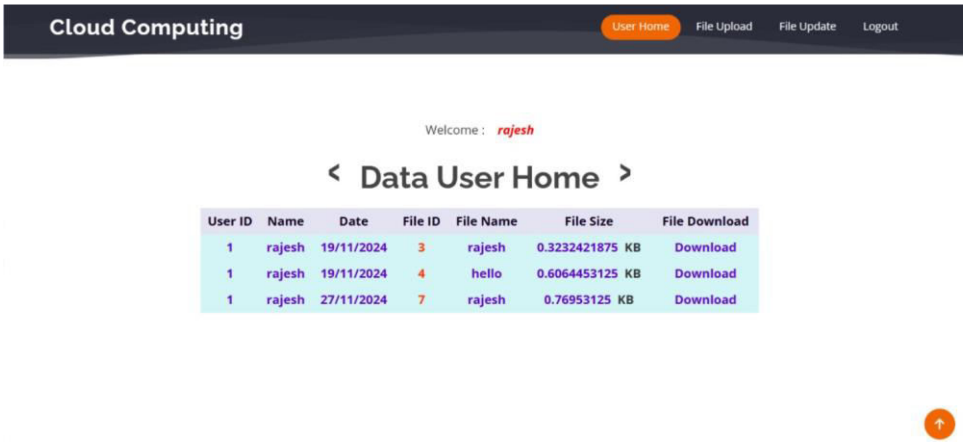
File Checking

File Name : rajesh File size : 0.3076171875 KB
File Block1 : clo



File Checking

File Name : rajesh File size : 0.3076171875 KB
File Block1 : project title cloud and fog environment using data integrity audit is our mini project title cloud and fog environment using data integrity audit is our mini project title cloud and fog environment using data integrity audit is our min



Welcome : rajesh

Data User Home

User ID	Name	Date	File ID	File Name	File Size	File Download
1	rajesh	19/11/2024	3	rajesh	0.3232421875 KB	Download
1	rajesh	19/11/2024	4	hello	0.6064453125 KB	Download
1	rajesh	27/11/2024	7	rajesh	0.76953125 KB	Download

DOI:10.15680/IJARETY.2024.1106056

REFERENCES

1.W. Shi, J. Cao, Q. Zhang, Y. Li and L. Xu, "Edge computing: Vision and challenges", IEEE Internet Things J., vol. 3, no. 5, pp. 637-646, Oct. 2016.
2.J. Li, Y. Zhang, X. Chen and Y. Xiang, "Secure attribute-based data sharing for resourcelimited users in cloud computing", Comput. Secur., vol. 72, pp. 1-12, Jan. 2018.
3.Y. Deswarte, J.-J. Quisquater and A. Saïdane, "Remote integrity checking", Proc. Working Conf. Integrity Internal Control Inf. Syst., pp. 1-11, 2003.
4.H. Wang, D. He, A. Fu, Q. Li and Q. Wang, "Provable data possession with outsourced data transfer", IEEE Trans. Services Comput., vol. 14, no. 6, pp. 1929-1939, Nov. 2021.
5.C. C. Erway, A. Küpçü and C. Papamanthou, "Dynamic provable data possession", ACM Trans. Inf. Syst. Secur., vol. 17, no. 4, pp. 1-29, 2009.

IJARETY

INNO SPACE
SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर
NISCAIR

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 7.394

www.ijarety.in editor.ijarety@gmail.com