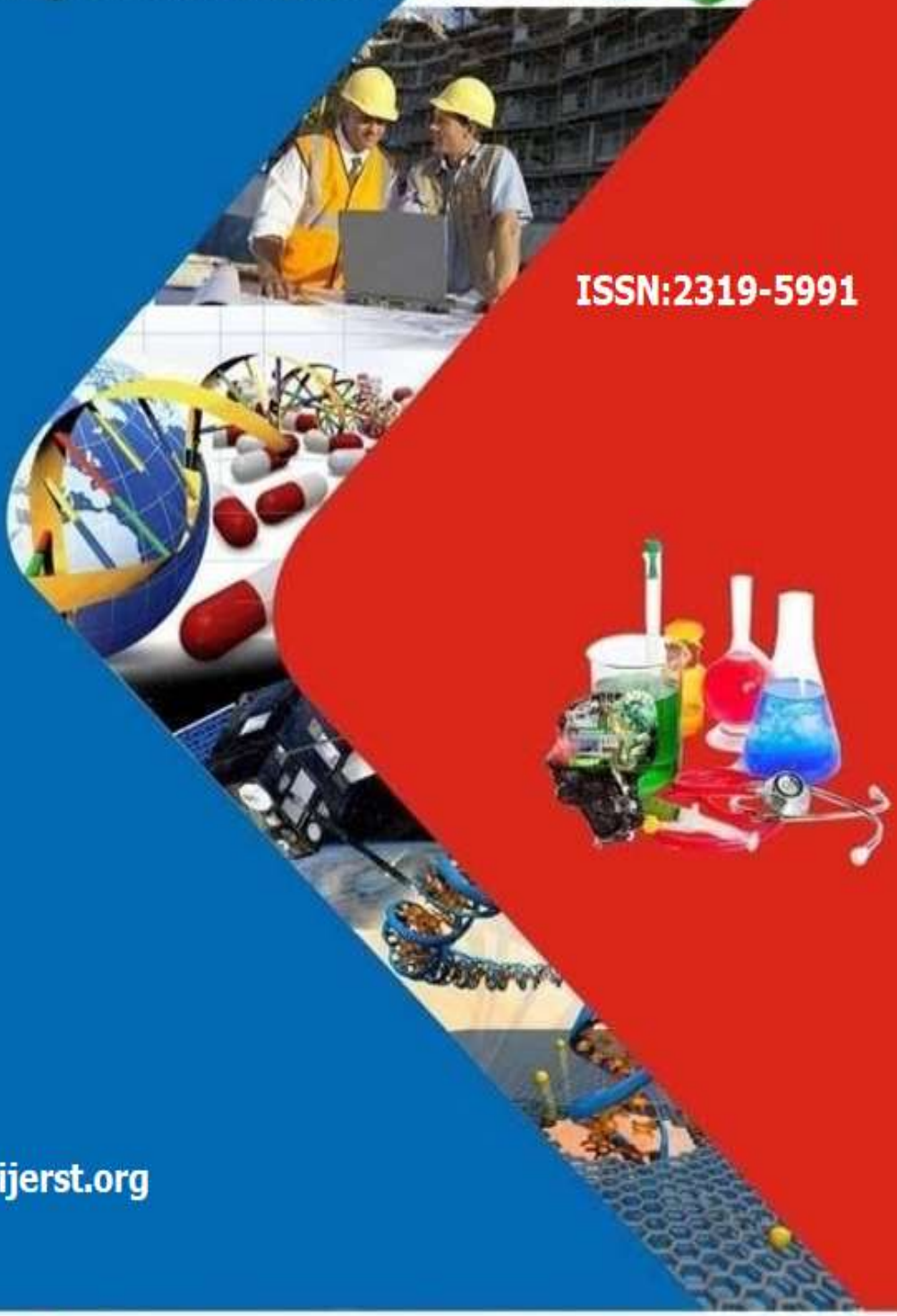
International Journal of Engineering Research and Science & Technology

IJERST

ISSN:2319-5991



www.ijerst.org

E-mail: editor@ijerst.org or ijerst.editor@gmail.com

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

PROTECTED INFORMATION MIGRATION AND REMOVAL VIA ENUMERATION BLOOMING FILTER IN CLOUD-BASED COMPUTING

1 Mrs. P. SWATHI, 2 S. SUMANTH, 3 T. THARANI, 4 SHARATH CHANDRA

5 S. PAVAN KUMAR, 6 D. SRUJAN REDDY

1Assistant Professor, Department of CSIT, Sri Indu College of Engineering and Technology-Hyderabad

2345Under Graduate, Department of CSIT, Sri Indu College of Engineering and Technology-Hyderabad

ABSTRACT

With the rapid development of cloud storage, an increasing number of data owners prefer to outsource their data to the cloud server, which can greatly reduce the local storage overhead. Because different cloud service providers offer distinct quality of data storage service, e.g., security, reliability, access speed and prices, cloud data transfer has become a fundamental requirement of the data owner to change the cloud service providers. Hence, how to securely migrate the data from one cloud to another and permanently delete the transferred data from the original cloud becomes a primary concern of data owners. To solve this problem, we construct a new counting Bloom filter-based scheme in this paper. The proposed scheme not only can achieve secure data transfer but also can realize permanent data deletion. Additionally, the proposed scheme can satisfy the public verifiability without requiring any trusted third party. Finally, we also develop a simulation implementation that demonstrates the practicality and efficiency of our proposal.

Keywords**: Cloud storage, Data deletion, Data transfer, Counting Bloom filter, Public verifiability**

I. INTRODUCTION

Cloud computing, an emerging and very promising computing paradigm, connects large-scale distributed storage resources, computing resources and network bandwidths together. By using these resources, it can provide tenants with plenty of high-quality cloud services. Due to the attractive advantages, the services (especially cloud storage service) have been widely applied, by which the resource-constraint data owners can outsource their data to the cloud server, which can greatly reduce the data owners' local storage overhead. According to the report of Cisco, the number of Internet consumers will reach about 3.6 billion in 2019, and about 55 percent of them will employ cloud storage service.

Because of the promising market prospect, an increasing number of companies (e.g., Microsoft, Amazon, Alibaba) offer data owners cloud storage service with different prices, security, access speed, etc. To enjoy more suitable cloud storage service, the data owners might change the cloud storage service providers. Hence, they might migrate their outsourced data from one cloud to another, and then delete the transferred data from the original cloud. According to Cisco, the cloud traffic is expected to be 95% of the total traffic by

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

the end of 2021, and almost 14% of the total cloud traffic will be the traffic between different cloud data centers. Foreseeably, the outsourced data transfer will become a fundamental requirement from the data owners' point of view.

To realize secure data migration, an outsourced data transfer app, Cloudsfer, has been designed utilizing cryptographic algorithm to prevent the data from privacy disclosure in the transfer phase. But there are still some security problems in processing the cloud data migration and deletion. Firstly, for saving network bandwidth, the cloud server might merely migrate part of the data, or even deliver some unrelated data to cheat the data owner. Secondly, because of the network instability, some data blocks may lose during the transfer process. Meanwhile, the adversary may destroy the transferred data blocks. Hence, the transferred data may be polluted during the migration process.

In short, the cloud storage service is economically attractive, but it inevitably suffers from some serious security challenges, specifically for the secure data transfer, integrity verification, verifiable deletion. These challenges, if not solved suitably, might prevent the public from accepting and employing cloud storage service.

Contributions In this work, we study the problems of secure data transfer and deletion in cloud storage, and focus on realizing the public verifiability. Then we propose a counting Bloom filter-based scheme, which not only can realize provable data transfer between two different clouds but also can achieve publicly verifiable data deletion. If the original cloud server does not migrate or remove the data honestly, the verifier (the data owner and the target cloud server) can detect these malicious operations by verifying the returned transfer and deletion evidences. Moreover, our proposed scheme does not need any Trusted third party (TTP), which is different from the existing solutions. Furthermore, we prove that our new proposal can satisfy the desired design goals through security analysis. Finally, the simulation experiments show that our new proposal is efficient and practical.

II. LITERATURE SURVEY

Storing data in encrypted form on servers like mail or file servers helps protect privacy and security. However, this often means giving up some functionality, such as being able to search for specific words in the data. In the past, it wasn't clear how to let servers perform these searches without exposing the data. This paper presents cryptographic methods that solve this problem by allowing searches on encrypted data while keeping the content secure. These methods offer several important benefits: the server cannot learn anything about the original data from the encrypted version, it can only see the results of specific searches, and it cannot search for anything without the user's permission. Additionally, users can search for a word without revealing what that word is to the server.

With the rise of pay-as-you-use cloud computing, many cloud services are now available to users. This makes things easier for people using smart devices, but also creates the challenge of finding the most suitable services or products. So, having

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

an intelligent and efficient cloud search system is very important.

To protect privacy, sensitive data is usually encrypted before being stored in the cloud. While current searchable encryption methods let users search this encrypted data, they only support exact keyword matches, which limits how useful the data is. Also, these methods don't guarantee that the search results are complete or correct. Sometimes, to save time or reduce data usage, cloud servers might only do part of the search or return incomplete results, which raises trust and reliability concerns.

Cloud computing is becoming more popular, and to protect privacy, sensitive data must be encrypted before being stored. However, this makes traditional plaintext keyword search ineffective. Existing searchable encryption methods only support exact or fuzzy keyword searches and do not handle semantic multi-keyword ranked search. In real scenarios, users often search using synonyms instead of exact terms due to content variation or lack of precise knowledge..

III. SYSTEM ANALYSIS

EXISTING SYSTEM

we study the problems of secure data transfer and deletion in cloud storage, and focus on realizing the public verifiability. Then we propose a counting Bloom filter-based scheme, whichnot only can realize provable data transfer between two different clouds but also can achieve publicly verifiable data deletion. If the original cloud server does not migrate or remove the datahonestly, the verifier (the data owner and the target cloud server) can detect these malicious operations by verifying the returned transfer and deletion evidences. Moreover, our proposed scheme does not need any Trusted third party (TTP), which is different from the existing solutions. Furthermore, we prove that our new proposal can satisfy the desired design goals through security analysis. Finally, the simulation experiments show that our new proposal is efficient and practical.

DISADVANTAGES OF EXISTING SYSTEM:

1.False Positives/Negatives: Enumeration Bloom Filters can result in false positives, causing unintended data removal, and false negatives, leaving sensitive data behind during migration or removal.

2.Limited Accuracy: The approach may struggle to achieve high precision and recall rates, leading to potential data remnants or unnecessary data movement.

3.Performance Impact: Enumeration Bloom Filters introduce computational overhead, impacting system performance and scalability, especially in large- scale cloud environments.

PROPOSED SYSTEM

We aim to achieve verifiable data transfer between two different clouds and reliable data deletion in cloud storage. Hence, three entities are included in our new construction,

In our scenario, the resource-constraint data owner might outsource his large-scale data to the cloud server A to greatly reduce the local storage overhead. Besides, the data owner might require the cloud A to move some data to the cloud B, or delete some data from the storage medium. The cloud A and cloud B provide the data owner with cloud storage service. We assume that the cloud A is the original cloud, which will be required to migrate

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

some data to the target cloud B, and remove the transferred data. However, the cloud A might not execute these operations sincerely for economic reasons. because they belong to two different companies. Hence, the two clouds will independently follow the protocol. Furthermore, we assume that the target cloud B will not maliciously slander the original cloud.

ADVANTAGES OF PROPOSED SYSTEM

1)Data confidentiality: The outsourced file may contain some private information that shouldbe kept secret. Hence, to protect the data confidentiality, the data owner needs to use secure algorithms to encrypt the file before uploading it to the cloud server.

2)Data integrity: The cloud A might only migrate part of the data, or deliver some unrelated data to the cloud B. Besides, the data might be polluted during the transfer process. Hence, the data owner and the cloud B should be able to verify the transferred data integrity to guarantee that the transferred data is intact.

3)Public verifiability: The cloud A may not move the data to the cloud B or delete the data faithfully. So, the verifiability of the transfer and deletion results should be satisfied from the data owner's point of view.

IV. IMPLEMENTATION

MODULE DESCRIPTION

1. Data Owner:

Responsibilities:

Initiates the data transfer process:--

The Data Owner is responsible for initiating the transfer of data between cloud service providers. This involves deciding which data to transfer and when.

Manages access control and permissions:-

Controls and specifies who has access to the data stored in the cloud. This includes setting access levels, permissions, and security policies to safeguard sensitive information.

Ensures security and privacy:-

Takes measures to guarantee the security and privacy of the data during both the transfer process and storage in the cloud. This involves implementing encryption, secure authentication, and other security protocols**.**

Tasks:

Requests data transfer:

Actively initiates the process of transferring data between cloud service providers based on specific needs or requirements.

Specifies security preferences and access control policies:

Defines the security preferences, access control policies, and any specific requirements for the data transfer to ensure compliance with security standards.

Verifies success of data migration and deletion processes:

Validates that the data has been successfully migrated to the new cloud and ensures that the original data in the old cloud is permanently deleted as per the request.

2.Cloud:

Responsibilities:

Stores and manages transferred data:

Manages the storage of data transferred by the Data Owner, ensuring it is stored securely and efficiently**.**

Ensures security, reliability, and accessibility:

Maintains the security and reliability of stored data, ensuring it is accessible to authorized users while protecting it from

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

unauthorized access or data loss. Collaborates in secure processes:

Actively collaborates in the secure transfer and deletion processes as initiated by the Data Owner. This collaboration involves implementing security measures to protect data during these operations**.**

Tasks:

Receives data transfer requests:

Listens for and receives data transfer requests from the Data Owner, acknowledging the need for data migration.

Implements secure data transfer mechanisms:

Utilizes secure mechanisms, potentially based on the counting Bloom filter scheme, to transfer data between cloud service providers while maintaining the confidentiality and integrity of the data.

Ensures permanent deletion of data:

- Guarantees the permanent deletion of data upon request from the Data Owner, ensuring that the information is irrecoverable and no longer stored in the cloud. Provides public Verifiability:
- Offers a mechanism for public verifiability, allowing stakeholders to independently verify the integrity and security of the data transfer without the need for a trusted third party.

Admin:

Responsibilities:

Manages and oversees the entire process:

Takes a holistic approach in managing and overseeing the data transfer and deletion process,ensuring it aligns with organizational policies and standards.

Monitors system security:

- Constantly monitors the security of the system, identifying and addressing any potential vulnerabilities or threats that may compromise the integrity of the data. Resolves issues
- Acts as a mediator and problem solver, resolving any issues that may arise during the data transfer or deletion processes, collaborating with both the Data Owner and Cloud as necessary.

Tasks:

Manages user accounts and access controls:

Administers user accounts and access controls, ensuring that only authorized personnel have the necessary permissions to manage and access the data.

Monitors performance and security:

Regularly monitors the performance and security of the cloud storage infrastructure, implementing any necessary updates or improvements to maintain optimal functionality.

Collaborates with stakeholders:

Collaborates with the Data Owner and Cloud to resolve conflicts or address any challenges that may emerge during the data transfer process.

Ensures public verifiability:

Establishes and maintains a system that allows for public verifiability of the data transfer, ensuring transparency and accountability without relying on a third party.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 2, 2025

V. RESULTS



HOME SCREEN



CLOUD A HOME PAGE



TRANSFERE DETAILS INTERFACE

VI. CONCLUSION

In conclusion, the proposed counting Bloom filter-based scheme addresses the critical issues of secure data transfer and deletion in cloud storage, with a focus on achieving public verifiability. The contributions of this work lie in its ability to provide provable data transfer between different cloud service providers and ensure publicly verifiable data deletion. The scheme offersa solution to challenges such as potential data manipulation, integrity verification, and the risk of malicious data retention by the original cloud server.

One key advantage of the proposed scheme is its independence from Trusted Third Parties (TTP), distinguishing it from existing solutions. By utilizing the counting Bloom filter, the scheme enables the data owner and the target cloud server to detect any dishonest migration or deletion operations through the verification of transfer and deletion evidence. This enhances the security and transparency of the data migration process, instilling confidence in data owners seeking to change cloud service providers.

The security analysis of the proposed scheme validates its ability to meet the desired design goals. Furthermore, simulation experiments demonstrate the efficiency and practicality of the proposal, reinforcing its viability in real-world applications. As cloud storage continues to play a pivotal role in modern computing, addressing security concerns associated with data transfer and deletion becomes imperative. The counting Bloom filter-based scheme presented in this work contributes significantly to the advancement of secure and verifiable data management in the cloud environment.

In essence, the proposed scheme not only aligns with the evolving landscape of cloud computing but also paves the way for more robust and trustworthy cloud storage services. Its innovative approach to data migration and deletion, coupled with the assurance of public verifiability, positions it as a valuable contribution to the field, providing a foundation for future developments in secure cloud data management.

REFERENCES

1. C. Yang and J. Ye, “Secure and efficient fine-grained data access control scheme in cloud computing”, Journal of High Speed Networks, Vol.21, No.4, pp.259–271, 2015.
2. X. Chen, J. Li, J. Ma, et al., “New algorithms for secure outsourcing of modular exponentiations”, IEEE

ISSN 2319-5991 www.ijerst.com
Vol. 21, Issue 2, 2025

Transactions on Parallel and Distributed Systems, Vol.25, No.9, pp.2386– 2396, 2014.

3. P. Li, J. Li, Z. Huang, et al., “Privacy-preserving outsourced classification in cloud computing”, Cluster Computing, Vol.21, No.1, pp.277–286, 2018.
4. B. Varghese and R. Buyya, “Next generation cloud computing: New trends and research directions”, Future Generation Computer Systems, Vol.79, pp.849–861, 2018.
5. W. Shen, J. Qin, J. Yu, et al., “Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage”, IEEE Transactions on Information Forensics and Security, Vol.14, No.2, pp.331–346, 2019.
6. R. Kaur, I. Chana and J. Bhattacharya J, “Data deduplication techniques for efficient cloud storage management: A systematic review”, The Journal of Supercomputing, Vol.74, No.5, pp.2035–2085, 2018.
7. Y. Liu, S. Xiao, H. Wang, et al., “New provable data transfer from provable data possession and deletion for secure cloud storage”, International Journal of Distributed Sensor Networks, Vol.15, No.4, pp.1–12, 2019.