ZKG INTERNATIONAL

ISSN: 2366-1313

Secure Data Transfer and Deletion from Counting Bloom Filter in Cloud Computing

1. Dr L K Sravanthi Potti 2. I Surya Sekhar 3. Ch Rudramadevi

Kodada Institute of Technology & Science for Women, Kodad, Telangana

Abstract- With the fast growth of cloud storage, a growing number of data owners are opting to outsource their data to a cloud server, which may significantly reduce local storage overhead. Because various cloud service providers provide varying levels of data storage service, such as security, dependability, access speed, and pricing, cloud data transfer has become a musthave for data owners looking to switch cloud service providers. As a result, data owners' major issue is how to safely migrate data from one cloud to another while also permanently deleting the transferred data from the original cloud. In this work, we propose a novel counting Bloom filter-based technique to tackle this problem. Not only can the suggested method provide safe data transport, but it can also ensure permanent data erasure. Furthermore, the suggested system may meet public verifiability requirements without the need of a trusted third party. Finally, we provide a simulation implementation to illustrate our proposal's feasibility and efficiency.

Key words — 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[1,2]. 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[3,4], 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[5,6]. According to the report of Cisco[7], the number of Internet consumers will reach about 3.6 billion in 2019, and about 55 percent of them will employ cloud storage service.

ISSN: 2366-1313

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[7], the cloud traffic is expected to be 95% of the total traffic by 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.

Cloud computing is the fusion and evolution of parallel computing, distributed computing, and grid computing as a new computer paradigm. Cloud storage is one of the most appealing cloud computing services because it allows customers to have convenient data storage and business access by connecting a large number of dispersed storage devices in a network. Users can outsource their data to a cloud server using cloud storage, which can significantly decrease local hardware/software overhead and human resource expenses. Cloud storage has become extensively used in everyday life and at business as a result of its appealing benefits. As a result, a growing number of resource-constrained customers, such as individuals and businesses, prefer to use cloud storage services. Because of the separation of outsourced data ownership and management, cloud storage unavoidably suffers from several additional security issues, such as data confidentiality, data integrity, data availability, and data erasure. These issues, particularly those related to data erasure, might stymie public adoption of cloud storage if not addressed properly. Data deletion, as the last step of the data life cycle, directly affects whether the data life cycle can be brought to a satisfactory conclusion, which is critical for data security and privacy preservation. Data deletion, on the other hand, receives far less attention than data integrity, which has been well researched and addressed. Although several verified deletion techniques for outsourced data in the cloud computing environment have been presented, there are still certain

ISSN: 2366-1313

issues and obstacles that need to be addressed immediately.

Cloud computing is a novel computing paradigm that combines and develops parallel computing, distributed computing, and grid computing. Cloud storage is one of the most appealing cloud computing services, as it may provide users with convenient data storage and business access services by connecting a large number of dispersed storage devices in a network. Users can outsource their data to the cloud server using cloud storage, which can significantly decrease local hardware/software overhead and human resource expenses. Cloud storage has become extensively used in everyday life and at business as a result of its appealing benefits. As a result, a growing number of resource-constrained customers, such as individuals and businesses, prefer to use cloud storage services [5], [6]. Because of the separation of outsourced data ownership and management, cloud storage unavoidably suffers from several additional security concerns, such as data confidentiality, data integrity, data availability, and data deletion. If these issues, particularly data erasure, are not addressed properly, public adoption of cloud storage may be hampered. Data deletion, as the final step of the data lifecycle, directly affects whether the data lifecycle can be brought to a satisfactory conclusion, which is critical for data security and privacy. Data deletion, on the other hand, receives far less attention than data integrity, which has been well researched and addressed. Although several verifiable deletion techniques for outsourced data in the cloud computing environment have been presented, there are still some issues and obstacles that need to be addressed thoroughly. To begin with, most existing methods are unable to provide fine-grained data erasure.

In general, data should be encrypted using a data key before being uploaded to a cloud server. As a result, theoretically, data deletion can be accomplished by deleting the relevant data decryption key, rendering the linked ciphertext inaccessible. Delete the datadecryption key, however, and the entire outsourced file will be unavailable. In most real-world applications, the user wishes to remove a portion of the data. In this instance, the user must update the entire outsourced file in order to delete a section, resulting in a significant computational and communication cost for both the user and the cloud server. As a result, fine-grained

ISSN: 2366-1313

outsourced data deletion techniques are needed, which should allow the user to delete some unnecessary data blocks flexibly.

II. RELATED WORK

Secure data deletion has been intensively investigated in recent decades, resulting in a plethora of literatures . Existing data deletion techniques may be divided into three categories based on the deletion methods used. The first technique for data deletion is unlinking, which is the most efficient and straightforward option. The file's link is specifically deleted from the underlying file system. After then, the user receives a one-bit response (Success or Failure) indicating the outcome of the data deletion process. Although unlinking effectively deletes a file's link, the file's content remains on the actual disc. As a result, the attacker may simply retrieve the "lost" data by using a tool to scan the relevant disc . As a result, the data deletion response may be misleading. Overwriting, which can destroy the file content, is the second way for deleting data. The basic concept is to replace the physical media with random data. Perito and Tsudik proposed a new technique called proofs of safe erasure in 2010. (PoSE-s). A series of random patterns is provided to overwrite the matching discs in their scheme. The identical string of patterns is then returned as proof of data deletion. Luo et al. [23] developed a unique outsourced data erasure technique that achieves the following: The Creative Commons Attribution 4.0 License applies to this work. See https://creativecommons.org/licenses/by/4.0/ for more details.

This paper has been accepted for publication in a future edition of this journal, but it is still being edited. Before the final publishing, the content may change. Yang et al., Publicly Verifiable and Efficient Fine-Grained Data Deletion Scheme in Cloud Computing, Yang et al., Publicly Verifiable and Efficient Fine-Grained Data Deletion Scheme in Cloud Computing, DOI10.1109/ACCESS.2020.2997351, IEEE AccessC. Yang et al., Publicly Verifiable By replacing the data with some random data, the data may be deleted. That is, the overwriting activity was camouflaged as a data update process. Meanwhile, they used a challenge-response mechanism to achieve data deletion resultchecking. However, owing to network delay, the verification may fail. Furthermore, overwriting deletion

ISSN: 2366-1313

has been specified in a number of standards (such as [24]). Destruction of the data decryption key is the third technique for data erasure. The basic concept is to destroy data encryption keys in order to make the ciphertext associated with them inaccessible. Boneh and Lipton introduced the first cryptography-based data erasure technique in 1996, and there have been several follow-up researches. Hao et al. presented a safe data-deletion method that stores the key in a trusted platform module (TPM).

III. 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 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 A.

Advantages-

1) Data confidentiality: The outsourced file may contain some private information that should be 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.

ISSN: 2366-1313

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

Secure Data Transfer And Deletion From Counting Bloom Filter In Cloud Computing

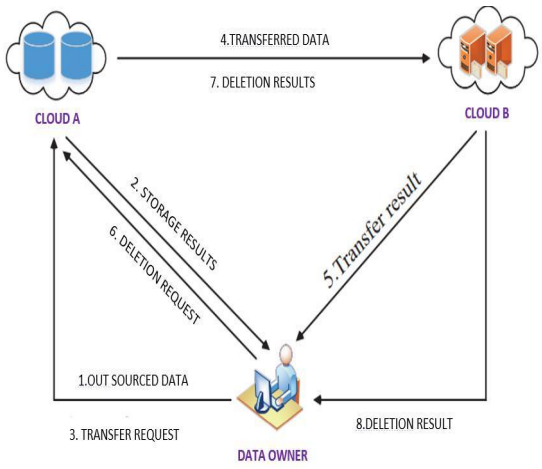
Objectives Proposed System

- To solve this problem, we propose a new counting Bloom filter-based scheme in this paper.

- The proposed scheme not only can achieve secure data transfer but also realize permanent data deletion.

- Additionally, the proposed scheme can satisfy the public verifiability without requiring any trusted third party. Here we use a new counting bloom filter-based scheme.

- The cloud storage service provider must authenticate the data owner.



Since such an outstanding data structure has been developed, improvement research based on it has been conducted, and a large number of studies have been published. There are more typical examples of the extended algorithm: Counting bloom filter solved the question of which elements cannot be deleted; Compressed Bloom filter uses arithmetic coding technique and ultimate entropy to compress BF vector as a message transfer in distributed system, resulting in a higher compression rate and

ISSN: 2366-1313

lower error rate; other improvement research includes: Spectral Bloom filter Bloom Filter is a very promising technology with a wide range of applications, according to a lot of improvement study. In the following practical application, Bloom Filter is mostly used to serve two roles.

(1) Because the Bloom Filter has space-saving properties, it may be used to replace largescale data with small-scale data, complete the judgement if an element is in the data set, express huge data sets, and enhance searching efficiency. This application mode focuses on database operations, dictionary queries, and file operations, as well as resource routing, packet routing, and network intrusion detection.

(2) Using the Bloom Filter method, the large scale raw data set is abstracted as abstract information, and the summary information is then communicated to other distributed nodes, such as a database. The transmission of the contents of the file directory information to each host in the distributed system is the most common use of this type.

IV. RESULTS

Fig-2 : Home Page

ISSN: 2366-1313

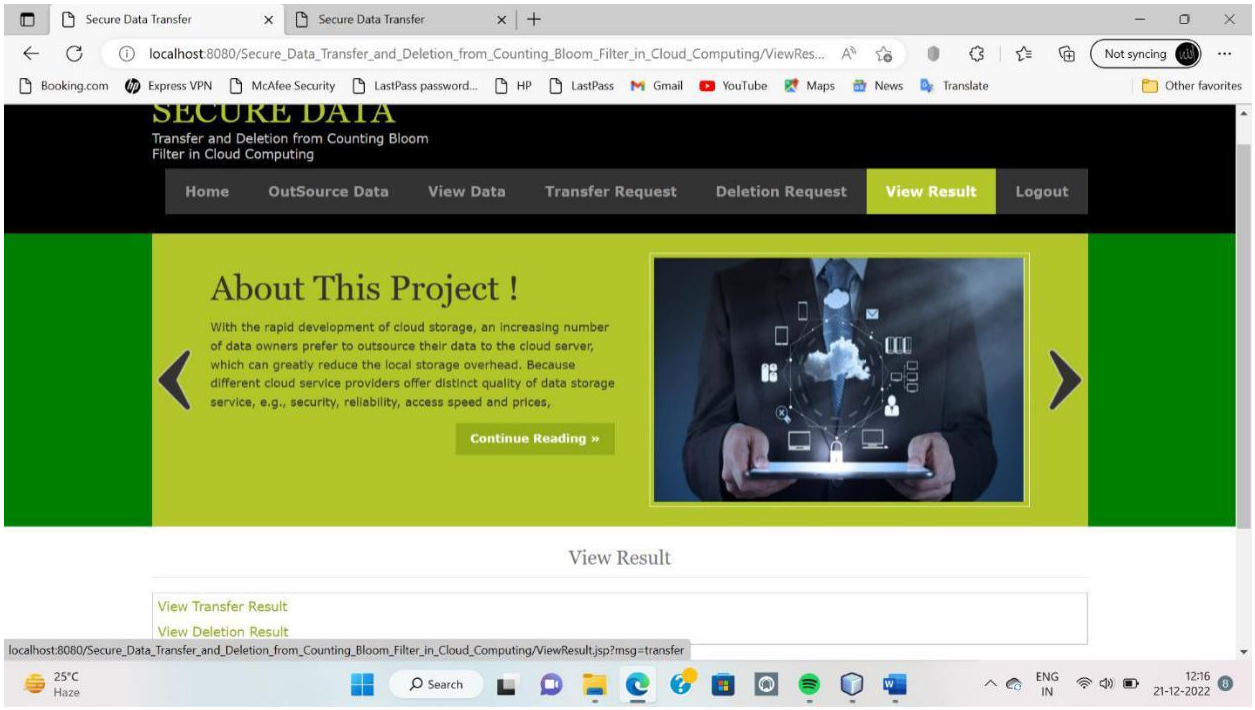


Fig-4 : View result page

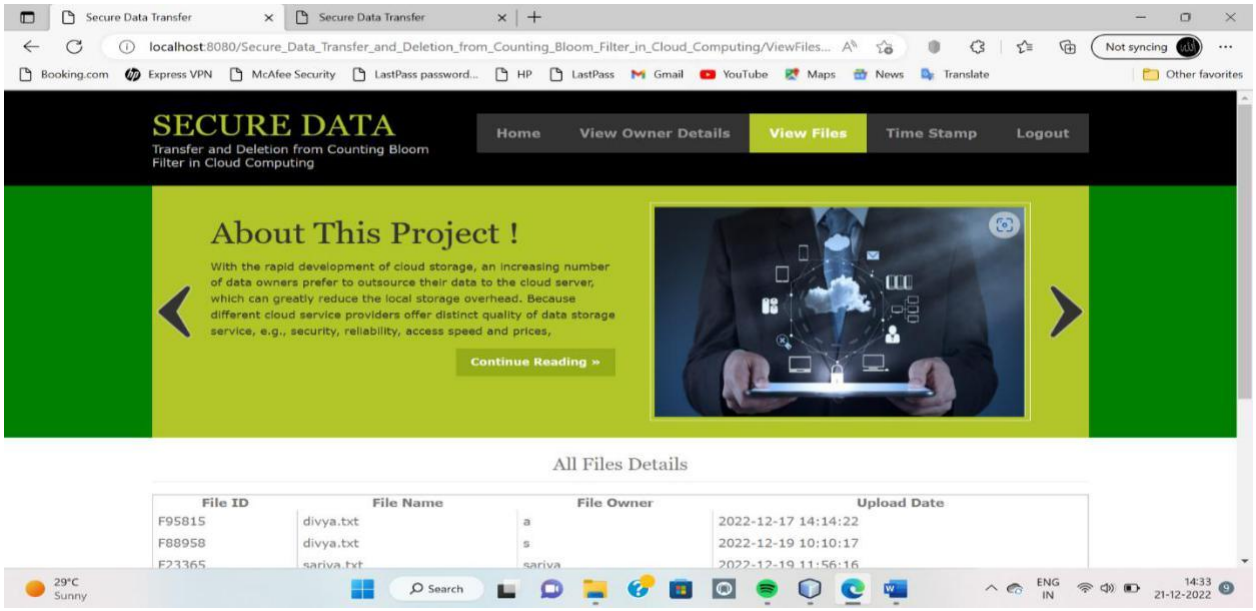


Fig-5. View files details

ISSN: 2366-1313

V. CONCLUSION

Conclusions The data owner in cloud storage does not think that the cloud server will carry out data transfer and delete activities honestly. We propose a CBF-based secure data transmission system that can also perform verified data erasure to overcome this challenge. In our system, cloud B may verify the integrity of the transmitted data, ensuring that the data is completely moved. Furthermore, cloud A should utilise CBF to produce a deletion proof after deletion, which would be used by the data owner to validate the deletion outcome. As a result, cloud A cannot act maliciously and effectively defraud the data owner. Finally, the results of the security analysis and simulation show that our solution is both secure and practical. Work in the future Our method, like all other systems, involves data transmission between two distinct cloud servers. With the advancement of cloud storage, the data owner may wish to transfer outsourced data from one cloud to two or more target clouds at the same time. However, the multi-target clouds might work together to defraud the data owner. As a result, we need to look at proving data transfer between three or more clouds. Future work Similar to all the existing solutions, our scheme considers the data transfer between two different cloud servers. However, with the development of cloud storage, the data owner might want to simultaneously migrate the outsourced data from one cloud to the other two or more target clouds. However, the multi-target clouds might collude together to cheat the data owner maliciously. Hence, the provable data migration among three or more clouds requires our further exploration.

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 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”,

ISSN: 2366-1313

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] Cisco, "Cisco global cloud index: Forecast and methodology, 2014–2019", available at:

https://www.cisco.com/c/en/us-/solutions/collateral/service-provider/global-cloud-index-gci/ white-paper-c11-738085.pdf, 2019-5-5.

[8] Cloudsfer, "Migrate & backup your files from any cloud to any cloud", available at: https://www.cloudsfer.com/, 2019-5-5.

[9] 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.

[10] Y. Wang, X. Tao, J. Ni, et al., "Data integrity checking with reliable data transfer for secure cloud storage", International Journal of Web and Grid Services, Vol.14, No.1, pp.106–121, 2018.

[11] Y. Luo, M. Xu, S. Fu, et al., "Enabling assured deletion in the cloud storage by overwriting", Proc. of the 4th ACM International Workshop on Security in Cloud Computing, Xi'an, China, pp.17–23, 2016.

ISSN: 2366-1313

[12] C. Yang and X. Tao, "New publicly verifiable cloud data deletion scheme with efficient tracking", Proc. of the 2th International Conference on Security with Intelligent Computing and Big-data Services, Guilin, China, pp.359–372, 2018.

[13] Y. Tang, P.P Lee, J.C. Lui, et al., "Secure overlay cloud storage with access control and assured deletion", IEEE Transactions on Dependable and Secure Computing, Vol.9, No.6, pp.903– 916, 2012.

[14] Y. Tang, P.P.C. Lee, J.C.S. Lui, et al., "FADE: Secure overlay cloud storage with file assured deletion", Proc. of the 6th International Conference on Security and Privacy in Communication
Systems, Springer, pp.380-397, 2010.

[15] Z. Mo, Y. Qiao and S. Chen, "Two-party fine-grained assured deletion of outsourced data in cloud systems", Proc. of the 34th International Conference on Distributed Computing Systems,

Madrid, Spain, pp.308–317, 2014.

[16] M. Paul and A. Saxena, "Proof of erasability for ensuring comprehensive data deletion in cloud computing", Proc. of the International Conference on Network Security and Applications,

Chennai, India, pp.340–348, 2010.