International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

Reliable and Effective Cloud Data Transfer Using Counting Bloom Filters

[1]Dr. R. VENKATA KRISHNA REDDY, [2]A. V. PHANI KUMAR, [3]C. VENKATA PAVAN KUMAR, [4]C. VENKATESWARLU

[1]Professor, Krishna Chaitanya Institute of Science & Technology, Kakuturu, Nellore, AP, India.

[2, 3,4]Assoc. Professor, Krishna Chaitanya Institute of Science & Technology, Kakuturu, Nellore, AP, India.

***Abstract* – Since cloud storage is developing so quickly, more and more data owners are choosing to outsource their data to cloud servers, which can significantly lower the overhead associated with local storage. Cloud data transfer has become a basic requirement for the data owner to switch cloud service providers because different providers offer varied quality of data storage services, such as security, reliability, access speed, and costs. Therefore, one of the main concerns of data owners is how to safely move data between clouds and erase the transferred data from the original cloud. In this study, we develop a novel counting Bloom filter-based approach to address this issue. The suggested plan can accomplish both permanent data deletion and secure data transfer. Furthermore, the suggested plan can meet public verifiability standards without the need for a reliable third party.**

***Index terms* – Bloom Filter, cloud storage, public verifiability, Data deletion.**

I. INTRODUCTION

The computing paradigm links network bandwidths, computer resources, and large-scale distributed storage resources [1,2]. It may offer a wide range of excellent cloud services to tenants by utilizing these resources. The services, particularly the cloud storage service, have been widely used because of its alluring benefits [3, 4]. Data owners with limited resources can use these services to outsource their data to the cloud server, which significantly lowers their local storage overhead [5, 6]. An estimated 3.6 billion people will use the Internet in 2019, and over 55% of them will use cloud storage services, according to a Cisco analysis [7].

A growing number of businesses (including Microsoft, Amazon, and Alibaba) are providing cloud storage services to data owners with varying costs, security levels, and speeds of access due to the market's potential future. The data owners may switch cloud storage service providers in order to benefit from better cloud storage services. Therefore, companies may move their data that is outsourced from one cloud to another and subsequently remove the data that was moved from the original cloud. By the end of 2021, cloud traffic is predicted to account for 95%

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

of all traffic, with traffic between cloud data centers accounting for about 14% of all cloud traffic, according to Cisco [7]. It is reasonable to assume that, from the perspective of the data owners, the transfer of data that is outsourced will become a basic necessity.

An outsourced data transfer application called Cloudsfer[8] was created using a cryptographic technique to prevent data privacy disclosure throughout the transfer process in order to achieve secure data migration. However, there are still certain security issues with the way cloud data deletion and migration are handled. First, the cloud server may just transfer a portion of the data or even provide irrelevant data to defraud the data owner in order to conserve network capacity [9]. Second, certain data blocks could be lost during the transmission process due to network instability.

The sent data blocks could be destroyed by the adversary in the interim [10]. As a result, throughout the migration procedure, the transferred data could become contaminated. Finally, the transferred data may be maliciously reserved by the originating cloud server for the purpose of uncovering the hidden advantages. From the perspective of the data owners, the data reservation is unanticipated. In summary, cloud storage services are cost-effective, but they unavoidably have significant security issues, particularly with regard to safe data transfer, integrity verification, and verifiable deletion. If these issues are not appropriately resolved, the general public may not accept and use cloud storage services.

II. BACKGROUND WORK

Numerous techniques have been developed as a result of extensive research on verifiable data erasure. After researching the objective of secure data deletion, Xue et al. [19] proposed an encryption technique based on key-policy attributes that can accomplish both assured deletion and fine-grained access control. They use the Merkle hash tree (MHT) to establish verifiability and remove the attribute to reach data deletion; nevertheless, their technique necessitates a trusted authority. In order to accomplish data integrity verification and proven deletion, Du et al. created the Associated deletion scheme for multi-copy (ADM), which makes use of pre-deleting sequence and MHT. To control the data keys, their scheme also needs a TTP. A Blockchain-based cloud data deletion technique was introduced by Yang et al. in 2018. The scheme involves the cloud performing the deletion operation and publishing the associated deletion proof on the blockchain. By confirming the deletion proof, any verifier can then examine the deletion result. Additionally, they remove the restriction caused by the need for a TTP. All of these techniques are capable of deleting data in a verifiable manner, but they are unable to ensure secure data transport.

Numerous techniques have been put out to move data between clouds and remove the transferred data from the original cloud. A Provable Data Possession (PDP) technique that can facilitate secure data migration was introduced

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

by Yu et al. in 2015. As far as we are aware, their plan is the first to effectively handle data transfer between two clouds; nevertheless, it is ineffective at deleting data because it does so by re-encrypting the transferred data, which necessitates a lot of information from the data owner. A proven data movement scheme with verifiable deletion and PDP was created by Xue et al. The data owner can use the Rank-based Merkle hash tree (RMHT) to confirm the deletion outcome and the PDP protocol to check the data integrity. Liu et al., however, identified a security vulnerability in the Ref. scheme and created a better plan that addresses the vulnerability. In order to provide a novel data transfer and deletion method that allows the data owner to confirm the transfer and deletion outcomes without requiring a TTP, Yang et al. implemented vector commitment in 2018. Additionally, their plan may verify data integrity on the target cloud.

III. PROPOSED SYSTEM

1. Overview

Verifiable data transfer and erasure are our goals in this scenario. Figure 1 illustrates the primary procedures. The first step is for the data owner to encrypt the data and send the ciphertext to cloud A. He then removes the local backup after verifying the storage outcome. Later, the data owner might move some data from cloud A to cloud B and switch cloud storage service providers. The data owner then want to verify the outcome of the transfer. Following a successful data transfer, the data owner needs cloud A to delete the transmitted data and verify the deletion outcome.

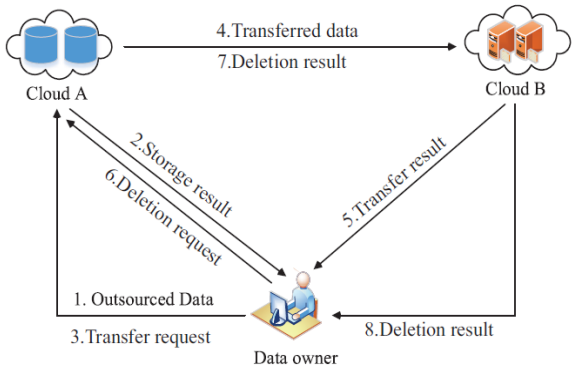

Fig. 1: the proposed System

2. The concrete scheme

The six algorithms listed below are part of our recently suggested strategy.

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

1) Initialization

Generate ECDSA public private key pairs (PK_O, SK_O), (PK_A, SK_A) and (PK_B, SK_B) for the data owner, the cloud A and the cloud B, respectively. Then the data owner chooses k secure hash functions g_1, g_2, · · · , g_k that all map any integer in [1,N] to distinct cells in CBF. Additionally, the data owner chooses a unique tag tag_f for the file that will be outsourced to the cloud A.

2) Data encryption

Before uploading, the data owner encrypts the outsourced file using a strong encryption process to preserve the confidentiality of the data.

3) Data outsourcing

D is stored in cloud A, which also produces storage proof. The data owner then removes the local backup after verifying the storage outcome.

4) Data transfer

The data owner moves selected data blocks, or possibly the entire file, from cloud A to cloud B when he wishes to switch service providers.

5) Transfer check

Cloud B returns the transfer result to the data owner after verifying that the transfer was successful.

6) Data deletion

After some data blocks have been successfully moved to cloud B, the data owner may request that cloud A remove them.

Implementation Modules

Multicloud: There are many data centers spread out over the globe, and a region like America or Asia typically has multiple data centers from the same or various cloud providers. In theory, a user in a certain area could access all of the data centers, but their performance would vary. Some data centers have extremely low latency, while others may have unacceptably high latency. Out of all the clouds that are available and meet the performance requirements—that is, those that can provide acceptable throughput and latency when not experiencing outages—the system selects one to store data.

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

Owner Module: Using an access policy, the owner module uploads their files. They obtain the public key for the specific upload file first, and then the owner requests the secret key for that specific upload file. The owner uploads their file using that secret key and executes Find out all the memory and cost details. View and buy the owner's virtual machines' details. Browse, encrypt, and upload the file. Verify the data integrity proof. Move data across clouds according to cost (Storage Mode Switching), Verify the price list and the cloud virtual machine details.

Cloud Storage: Services for cloud storage have grown in popularity. Given the significance of privacy, numerous encryption strategies for cloud storage have been put out to shield data from unauthorized access. In reality, some authorities (i.e., coercers) may force cloud storage providers to divulge user secrets or private information on the cloud, completely defeating storage encryption systems. All of these schemes were predicated on the idea that cloud storage providers are secure and impenetrable. In order to ensure user privacy, we propose in this paper our proposal for a new encryption system for cloud storage that allows cloud storage providers to fabricate convincing false user secrets.

User Module: Using the file name and file ID, this module assists the client in searching the file. The user will not receive the file if the file name and ID are incorrect; otherwise, the server will request the secret key and obtain the encrypted file. The user has the secret key and uses it if they wish to decrypt the file. View every assailant, View Resource Utilization Profiles, which show the total amount of memory consumed by each data owner. View all of the VM and pricing information, Pointing of the Resource Migration Check (if it surpasses the threshold).

IV. RESULTS AND DISCUSSION

Data confidentiality

Without the matching data decryption key, an attacker cannot obtain any plaintext information due to data secrecy. The data owner encrypts the file in our approach using the IND-CPA safe AES algorithm. In the meantime, the data decryption key is calculated as follows: k = H(tagf ||SKO), where SKO is the secret private key and H is a secure hash function. As a result, the attacker is unable to successfully manufacture a legitimate data decryption key. Additionally, the data owner maintains the confidentiality of the data decryption key. In other words, no opponent can get the decryption key to access the plaintext data further.

Data integrity

The transferred data must be intact in order for cloud B to accept it. This is known as data integrity. Cloud B validates the equation Hi = H(tagf ||ai||Ci), where i ∈ ϕ, after receiving the transmitted data (ai,Ci) from cloud A and the hash values Hi from the data owner. Keep in mind that the data owner uses a secure hash algorithm to calculate

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

{Hi}i∈ϕ. In order for the equation Hi = H(tagf ||ai||C′ i) to hold, cloud A and other adversaries are unable to create a new data block (ai,C′ i).

In other words, cloud B is able to recognize malicious activity and will reject the received data if cloud A fails to migrate the data to cloud B honestly or if the attackers alter the transmitted data blocks during the migration process. As a result, the transferred data's integrity is assured.

Public verifiability

The verifiability of the deletion result and the transfer result are examined, respectively. The transfer outcome can be confirmed by the verifier who possesses the transfer evidence π and the transfer request Rt. In particular, the verifier first determines whether Rt is valid. The data owner did, in fact, request that the data be moved to cloud B if Rt is legitimate. The verifier then confirms that the signatures sigta and sigtb are legitimate. It should be noted that cloud B will not intentionally conspire with cloud A to deceive the data owner. Hence, the verifier can trust the returned transfer result if and only if both the signatures are legitimate. Additionally, by confirming the counting Bloom filter CBFb, the verifier determines whether cloud B honestly maintains the transferred data.

Experimental Setup

In this project, we create a web application using Java technology, a database using MySQL, and the necessary hardware. CPU with two cores and two gigabytes of RAM. We put our suggested technique for safe data deletion and transfer into practice using the aforementioned technology.

Experimental Results

Fig. 2: Home Page

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

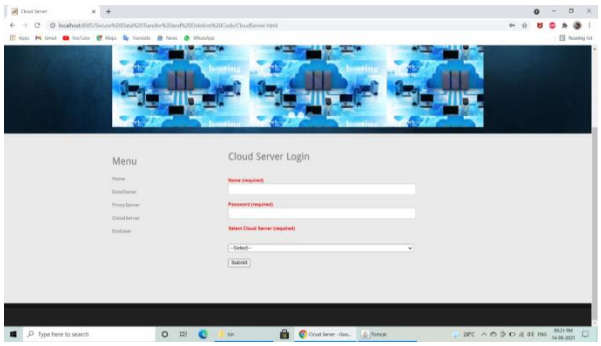

Fig. 3: Cloud Server Login

Fig. 4: Cloud Files

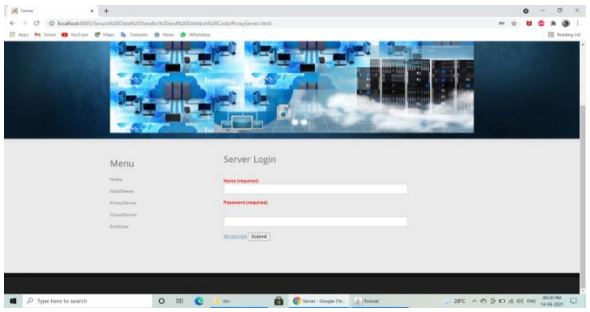

Fig. 5: Proxy Server Login

International journal of basic and applied research

www.pragatipublication.com

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

Fig. 6: Migrated File details

V. CONCLUSION

The owner of the data does not trust that the cloud server would carry out the data destruction and transfer processes in an honest manner. We suggest a CBF-based secure data transfer mechanism that can also achieve verified data deletion in order to address this issue. In our plan, cloud B can ensure that the data is fully moved by verifying the integrity of the transferred data. Additionally, cloud A should employ CBF to produce deletion evidence following deletion, which the data owner will use to confirm the deletion outcome. Therefore, cloud A is unable to act maliciously and successfully defraud the data owner.

REFRENCES

[1] C. Yang and J. Ye, "Secure and efficient fine-grained dataaccess control scheme in cloud computing", Journal of HighSpeed Networks, Vol.21, No.4, pp.259–271, 2015.

[2] X. Chen, J. Li, J. Ma, et al., "New algorithms forsecure outsourcing of modular exponentiations", IEEETransactions on Parallel and Distributed Systems, Vol.25,No.9, pp.2386–2396, 2014.

[3] P. Li, J. Li, Z. Huang, et al., "Privacy-preserving outsourcedclassification 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 GenerationComputer Systems, Vol.79, pp.849–861, 2018.

[5] W. Shen, J. Qin, J. Yu, et al., "Enabling identity-basedintegrity auditing and data sharing with sensitive informationhiding for secure cloud storage", IEEE Transactions on InformationForensics and Security, Vol.14, No.2, pp.331–346,2019.

[6] R. Kaur, I. Chana and J. Bhattacharya J, "Data deduplicationtechniques for efficient cloud storage management: Asystematic review", The Journal of Supercomputing, Vol.74,No.5, pp.2035–2085, 2018.

ISSN 2249-3352 (P) 2278-0505 (E)

Cosmos Impact Factor-5.86

[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 anycloud", available at: https://www.cloudsfer.com/, 2019-5-5.

[9] Y. Liu, S. Xiao, H. Wang, et al., "New provable datatransfer from provable data possession and deletion for securecloud storage", International Journal of Distributed SensorNetworks, Vol.15, No.4, pp.1–12, 2019.

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