Secure Data Transmission and Deletion between Two Clouds without Overhead

Syed Ehtesham Ali, Kushboo Tackiar, P. Nitheesha, BE VIII SEM, CSE,
Dr. V. Padmakar, Associate Professor, CSE,Sandeep Ravikanti,Assistant professor,CSE
Methodist college of Engineering and Technology, Abids, Hyderabad, 500001

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.*

Keywords: Cloud storage, Data transfer, Data deletion, Counting bloom filter, Public verifiability.

I.INTRODUCTION

Cloud computing, an emerging and very promising computing paradigm[1], 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 owner's local storage overhead. According to the report of Cisco, the number of Internet consumers will reach about 3.6 billion[6] 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 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 owner's 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. Last but not least, the original cloud server might maliciously reserve the transferred data for digging the implicit benefits. The data reservation is unexpected from the data owners point of view. 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[2]. These challenges, if not solved suitably, might prevent the public from accepting and employing cloud storage service.

II. LITERATURE SURVEY

A verifiable data deletion has been well studied for a long time, resulting in many solutions. Xue et al. studied the goal of secure data deletion and put forward a key-policy attribute-based encryption scheme, which can achieve data finegrained access control and assured deletion. They reach data deletion by removing the attribute and use Merkle hash tree (MHT) to achieve verifiability, but their scheme requires a trusted authority. Du et al. designed a scheme called Associated deletion scheme for multi-copy (ADM)[3], which uses pre-deleting sequence and MHT to achieve data integrity verification and provable deletion. However, their scheme also requires a TTP to manage the data keys. In 2018, Yang et al. presented a Block chain-based cloud data deletion scheme, in which the cloud executes deletion operation and publishes the corresponding deletion evidence on Blockchain. Then any verifier can check the deletion result by verifying the deletion proof. Besides, they solve the bottleneck of requiring a TTP.

Although these schemes all can achieve verifiable data deletion, they cannot realize secure data transfer. To migrate the data from one cloud to another and delete the transferred data from the original cloud, many methods have been proposed. In 2015, Yu et al. presented a Provable data possession (PDP) scheme that can also support secure data migration. To the best of our knowledge, their scheme is the first one to solve the data transfer between two clouds efficiently, but it's inefficient in data deletion process since they reach deletion by re-encrypting the transferred data, which requires the data owner to provide many information. Xue et al. designed a provable data migration scheme, which characterized by PDP and verifiable deletion. The data owner can check the data integrity through PDP protocol and verify the deletion result by Rank-based Merkle hash tree (RMHT)[4]. However, Liu et al. pointed out that there exists a security flaw in the scheme and they designed an improved scheme that can solve the security flaw. In 2018, Yang et al. adopted vector commitment to design a new data transfer and deletion scheme, which offers the data owner the ability to verify the transfer and deletion results without any TTP. Moreover, their scheme can realize data integrity verification on the target cloud.

2. System Working

The system works on the concept of 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[3]. Our proposed scheme does not need any Trusted third party (TTP), which is different from the existing solutions.Our new proposal can satisfy the desired design goals through security analysis. The activity diagram can be seen in **fig 2.1.1** and class diagram can be seen in **fig 2.1.2**

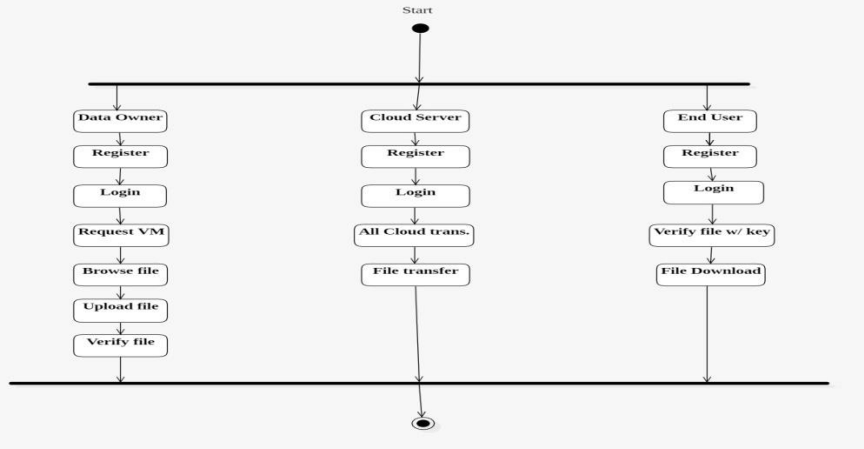

Fig 2.1.1 Activity Diagram

The behavioural diagram portrays the control flow from a start point to a finish point and taking various decision paths that exist while the activity is being executed.

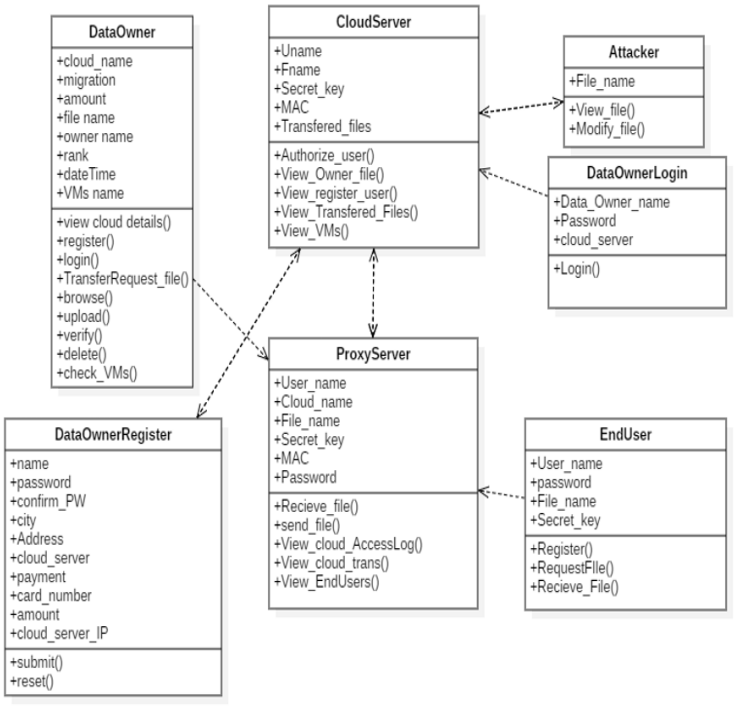

Fig 2.1.2 Class Diagram

As shown in above fig 2.1.2, these are the main building block in object-oriented which shows different attributes and methods(operations) and the relationship among data owner depending upon cloud server's, proxy server's and end user's functionalities. The attacker can attack on cloud server to view and modify data i.e, hack the server and misuse or steal the data. For registration different classes are defined considering all the attributes.

2.1 Algorithms

Counting Bloom Filter (CBF):

Bloom filter (BF)[1], a space-efficient data structure, conceived by Burton Howard Bloom in 1970, that is used to test that if a set contains a specified element. This designed to tell, rapidly and memory-efficiently, whether an element is present in a set. BF costs constant time overhead to insert an element or verify that whether an element belongs to the set, no matter how many elements the set and the BF includes. A BF initially represents a bit of array of m bits, all set to 0.

The insertion takes an element and inputs it to k different hash functions each mapping the element to one of the m array positions, which are then set to 1. When querying the BF on a element, it is considered to be in the BF if all positions obtained by evaluating the hash evaluations are set to 1. The initial secret key sk output by the generation algorithm of a BFE scheme corresponds to an empty BF. Encryption takes a message M and the public key pk, samples a random element s (acting as a tag for the ciphertext) corresponding to the universe U of the BF and encrypts a message using pk with respect to the k positions set in the BF by s.

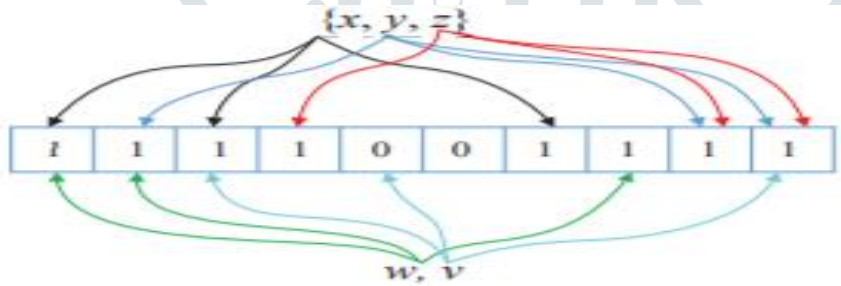

Fig 2.2.1 Example of Bloom filter

A BF can be viewed as a m length bit array with k hash functions: hi(·) : {0, 1} ∗ → {0, 1, …… ... , m}. To insert an element, we need to set the group of k bits to 1, the positions of thesebits are determined by hash values h1(x), ……... ,hk(x). Membership tests are implemented by executing the same hash calculations and outputting success if all of the correspondingpositions are one, as shown in Fig 2.2.1.

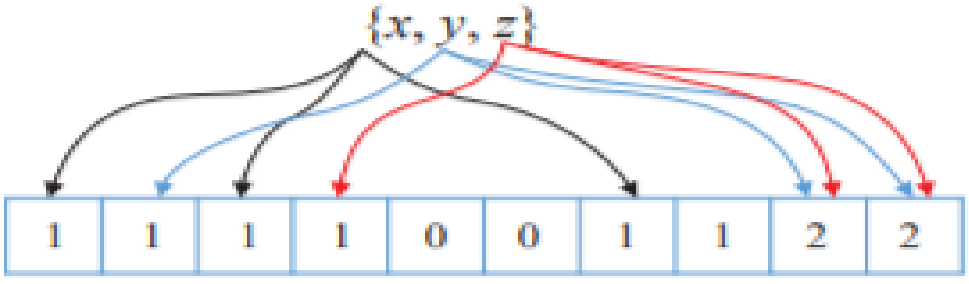

Fig 2.2.2 Example of Counting Bloom filter

Note that there is a false positive in the BF, which means that even all the k bits related to w are one, but w does not belong to the set with a small probability.

However, we can choose appropriate parameters to reduce the probability, e.g., the number of the hash functions k, the length of the BF m and the number of the elements n . Further, the probability will be so small that it can be negligible if the parameters are suitable. Besides, BF cannot delete an element from the data set. To solve this drawback, Counting Bloom filter (CBF) is presented. As a variant of BF, CBF uses a counter cell count to replace every "bit" position, as illustrated in Fig 2.2.2 To insert an element y, we require to increase the k related counters by one, the indexes of the counters are also determined by the hash values

h1(y), h2(y), · · · , hk(y). On the contrary, the element deletion operation is simply to decrease the k Secure Data Transfer and Deletion from Counting Bloom Filter in Cloud Computing 275 corresponding counters by one.

AES Algorithm:

Advanced Encryption Standards (AES) is a symmetric-key algorithm. MAC uses block cipher algorithm. A block cipher is an algorithm that encrypts and decrypts the data using 128/192/256-bit keys into 128-bit blocks.Symmetric key algorithms are sometimes referred to as secret key algorithms. This is because these types of algorithms generally use one key that is kept secret by the systems engaged in the encryption and decryption processes. Symmetric key algorithms are algorithms for cryptography[6] that use the same cryptographic keys for both the encryption of plain text and the decryption of cipher text.

The keys may be identical, or there may be a simple transformation to go between the two keys. The keys, in practice represent a shared secret between two or more parties that can be used to maintain a private information link. The requirement that both parties' have access to the secret key is one of the main drawbacks of symmetric-key encryption, in comparison to public-key encryption (Also known as asymmetric-key encryption).

III.MODULES USED

Multi Cloud: Multi-cloud[7] is a strategy where an organization leverages two or more cloud computing platforms to perform various tasks. Organizations that do not want to depend on a single cloud provider may choose to use resources from several providers to get the best benefits from each unique service.

Data Owner: Data owners are either individuals or teams who make decisions such as who has the right to access and edit data and how it's used. Owners may not work with their data every day, but are responsible for overseeing and protecting a data domain.

Cloud Storage: Cloud Storage is delivered on demand with just-in-time capacity and costs, and eliminates buying and managing your own data storage infrastructure. This gives you agility, global scale and durability, with "anytime, anywhere" data access.Cloud storage is purchased from a third party cloud vendor who owns and operates data storage capacity and delivers it over the Internet in a pay-as-you-go model.

Owner: Owner module is to upload their files using some access policy. First they get the public key for particular file upload after getting this public key owner request the secret key for particular upload file. Using that secret key owner upload their file and performs find all cost and memory details, view owner's VMs details and purchase, browse and encrypts file and upload, check data integrity proof, transfer data from one to another cloud based on the price (Storage Mode Switching), check all cloud VM details and price list.

End user: This module is used to help the client in searching a file using file id and file name. If the file id and name are incorrect, the user cannot the file. Otherwise, server asks the .secret key and gets the encryption file.

IV.IMPLEMENTATION

4.1 Technologies Used

Java: Java is a free-to-use and platform independent programming language that's also open source. Java is primarily used for Internet-based applications, Java is a simple, efficient, general-purpose language[5]. Java is quick to learn, making this a highly logical choice.It is a portable, object-oriented, interpreted language. Java is extremely portable.Java is also particularly known for its role in creating applications. Java runs on JVM. This essentially means it provides many developer-friendly mechanisms. Some of these include Code Optimisation, Memory Management, as well as the Garbage Collector function.

4.2 Working

The data owner uses Counting Bloom Filter, When the data owner wants to change the service provider, he migrates some data blocks, even the whole file from one cloud to the other cloud based on the services provided like resources, threshold VMs, prices and memory. On uploading the data, the data is encrypted that is cipher text is generated along with a secret key using AES algorithm. To transfer or access the data, secret key is required.

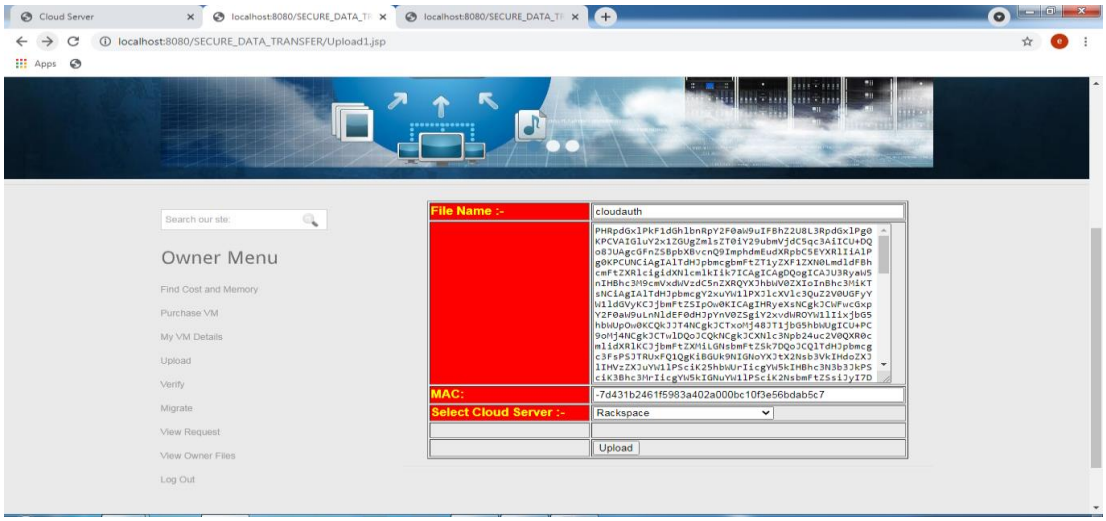

Fig 4.2.1 Encrypting the data

If user wants to transfer data, request is sent by the user to data owner. The data owner checks for the request and responds to the request by providing the secret key to transfer the data to other cloud. The other cloud wants to check the correctness of the transfer and returns the transfer result to the data owner. Iff all the verifications pass,the data owner trusts the transfer proof is valid, and the other cloud stores the transferred data honestly. On transfer, the file is downloaded. The data owner requires the previous cloud to delete some data blocks when they have been transferred to the other cloud successfully[8].

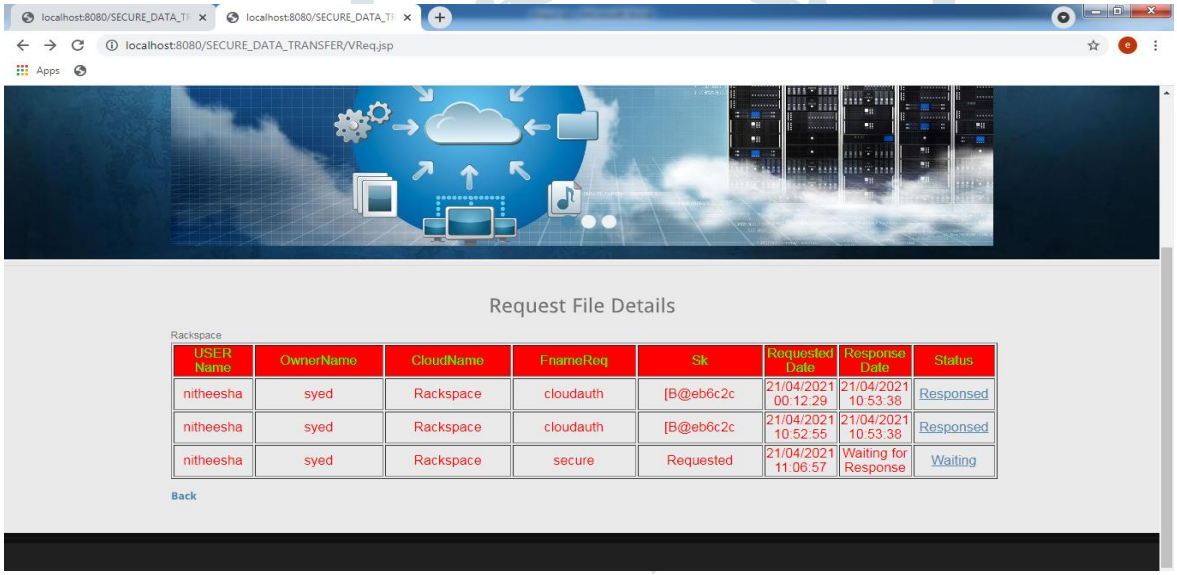

Fig 4.2.2 Request and response page

CONCLUSION AND FUTURE SCOPE

Conclusions In cloud storage, the data owner does not believe that the cloud server might execute the data transfer and deletion operations honestly. To solve this problem, we propose a CBF-based secure data transfer scheme, which can also realize verifiable data deletion. In our scheme, the cloud B can check the transferred data integrity, which can guarantee the data is entirely migrated. Moreover, the cloud A should adopt CBF to generate a deletion evidence after deletion, which will be used to verify the deletion result by the data owner. Hence, the cloud A cannot behave maliciously and cheat the data owner successfully. Finally, the security analysis and simulation results validate the security and practicability of our proposal, respectively.

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[7] 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. Cloudsfer, "Migrate & backup your files from any cloud to any cloud", available at: *https://www.cloudsfer.com/*, 2019-5-5.
3. 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.
4. J. Wang, X. Chen, X. Huang, *et al*., "Verifiable auditing for outsourced database in cloud computing", *IEEE transactions on computers*, Vol.64, No.11, pp.3293–3303, 2015.
5. Sandeep ravikanti, An IoT & AWS Based Smart Door Authentication System for Securing Hospital Maternity Wards,Volume-65 Number-1,10.14445/22312803/IJCTT-V65P102
6. Sandeep Ravikanti , Dheeraj Ganesh, Smart Farming: A Techno Agriculture Advancement Powered by Machine Learning,Volume 64 Number 1 – October 2018
7. Sandeep Ravikanti,classification model to predict dynamic healthcare resource utilization and allotment method by using cart analysis for surgical patients los, JETIR May 2021, Volume 8, Issue 5
8. Sandeep Ravikanti,Internet of Everything (IoE): A New Technology Era will have Impact on Every Facet of our Life,volume 4 issue 3.