Journal of Engineering Sciences

Vol 12, Issue 06, JUNE /2021
ISSN NO:0377-9254

A New Methodology Cloud- Bloom Filter Based On Efficient Privacy Preserving Data Deletion And Transfer

SIVANI MUDIYAM, MANJULA MUKKAMALLA, AMEENA BEE DUDEKULA, B RAMA SUBBAIAH, Dr.G RAJESH CHANDRA

DEPT OF CSE

SVR ENGINEERING COLLEGE, NANDYAL

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.

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. 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.

To realize secure data migration, an outsourced data transfer app, Cloudsfer[8], 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[9]. Secondly, because of the network instability, some data blocks may lose during the transfer process. Meanwhile, the adversary may destroy the transferred data blocks[10]. 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[11]. 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. 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. EXISTING SYSTEM:

- Xue *et al*.[19] studied the goal of secure data deletion, and put forward a key-policy attribute based encryption scheme, which can achieve data fine grained 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*.[20] designed a scheme called Associated deletion scheme for multi-copy (ADM), 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*.[21] presented a Blockchain-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.

Disadvantages

- In the existing work, the system does not provide **Data integrity proof**.
- This system is less performance due to lack of strong encryption techniques.

III. PROPOSED SYSTEM:

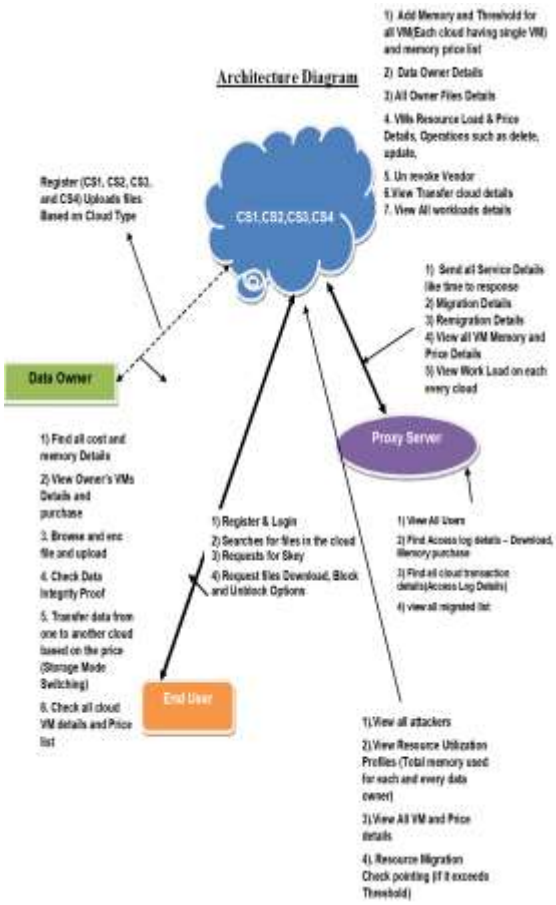
- In the proposed work, the system studies the problems of secure data transfer and deletion in cloud storage, and focus on realizing the public verifiability. Then the system proposes a counting Bloom filter-based scheme, which not only can realize provable data transfer between two different clouds 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.

Advantages

- **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.
- **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.

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. SYSTEM ARCHITECTURE:



V. MODULES:

- **Multi-cloud**:

Lots of data centers are distributed around the world, and one region such as America, Asia, usually has several data centers belonging to the same or different cloud providers. So technically all the data centers can be access by a user in a certain region, but the user would experience different performance. The latency of some data centers is very low while that of some ones may be intolerable high. System chooses clouds for storing data from all the available clouds which meet the performance requirement, that is, they can offer acceptable throughput and latency when they are not in outage. The storage mode transition does not impact the performance of the service. Since it is not a latency-sensitive process, we can decrease the priority of transition operations, and implement the transition in batch when the proxy has low workload.

- **Data Owner:**

In this section, we elaborate a cost-efficient data hosting model with high availability in heterogenous multi-cloud, named "MULTI CLOUD". The architecture of CHARM is shown in Figure 3. The whole model is located in the proxy in this system. There are four main components in MULTI CLOUD: Data Hosting, Storage Mode Switching (SMS), Workload Statistic, and Predictor. Workload Statistic keeps collecting and tackling access logs to guide the placement of data. It also sends statistic information to Predictor which guides the action of SMS. Data Hosting stores data using replication or erasure coding, according to the size and access frequency of the data. SMS decides whether the storage mode of certain data should be changed from replication to erasure coding or in reverse, according to the output of Predictor. The implementation of changing storage mode runs in the background, in order not to impact online service. Predictor is used to predict the future access frequency of files. The time interval for prediction is one month, that is, we use the former months to predict access frequency of files in the next month. However, we do not put emphasis on the design of predictor, because there have been lots of good algorithms for prediction. Moreover, a very simple predictor, which uses the weighted moving average approach, works well in our data hosting model. Data Hosting and SMS are two important modules in MULTI CLOUD. Data Hosting decides storage mode and the

clouds that the data should be stored in. This is a complex integer programming problem demonstrated in the following subsections. Then we illustrate how SMS works in detail in x V, that is, when and how many times should the transition be implemented.

- **Cloud Storage:**

Cloud storage services have become increasingly popular. Because of the importance of privacy, many cloud storage encryption schemes have been proposed to protect data from those who do not have access. All such schemes assumed that cloud storage providers are safe and cannot be hacked; however, in practice, some authorities (i.e., coercers) may force cloud storage providers to reveal user secrets or confidential data on the cloud, thus altogether circumventing storage encryption schemes. In this paper, we present our design for a new cloud storage encryption scheme that enables cloud storage providers to create convincing fake user secrets to protect user privacy. Since coercers cannot tell if obtained secrets are true or not, the cloud storage providers ensure that user privacy is still securely protected. Most of the proposed schemes assume cloud storage service providers or trusted third parties handling key management are trusted and cannot be hacked; however, in practice, some entities may intercept communications between users and cloud storage providers and then compel storage providers to release user secrets by using government power or other means. In this case, encrypted data are assumed to be known and storage providers are requested to release user secrets. we aimed to build an encryption scheme that could help cloud storage providers avoid this predicament. In our approach, we offer cloud storage providers means to create fake user secrets. Given such fake user secrets, outside coercers can only obtained forged data from a user's stored ciphertext. Once coercers think the received secrets are real, they will be satisfied and more importantly cloud storage providers will not have revealed any real secrets. Therefore, user privacy is still protected. This concept comes from a special kind of encryption scheme called deniable encryption.

- **Owner Module:**

Owner module is to upload their files using some access policy. First they get the public key for particular upload file 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 enc 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.

- **User Module:**

This module is used to help the client to search the file using the file id and file name. If the file id and name is incorrect means the user does not get the file, otherwise server ask the secret key and get the encryption file. If the user wants the decryption file means user have the secret key and performs View all attackers,View Resource Utilization Profiles (Total memory used for each and every data owner),View All VM and Price details,Resource Migration Check pointing (if it exceeds Threshold).

VI. SYSTEM SPECIFICATION:

H/W System Configuration:-

- Processor - Pentium –IV
- RAM - 4 GB (min)
- Hard Disk - 20 GB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA

Software Requirements:

- Operating System - Windows XP
- Coding Language - Java/J2EE(JSP,Servlet)
- Front End - J2EE

Back End - MySQL

VII. CONCLUSION:

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 our further exploration.

VIII. 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", *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.
[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.
[17] A. Rahumed, H.C.H. Chen, Y. Tang, *et al*., "A secure cloud
backup system with assured deletion and version control",
*Proc. of the 40th International Conference on Parallel
Processing Workshops*, Taipei City, Taiwan, pp.160–167,
2011.
[18] B. Hall and M. Govindarasu, "An assured deletion technique
for cloud-based IoT", *Proc. of the 27th International Conference on Computer Communication and Networks*,
Hangzhou, China, pp.1–8, 2018.
[19] L. Xue, Y. Yu, Y. Li, *et al*., "Efficient attributebased
encryption with attribute revocation for assured data
deletion", *Information Sciences*, Vol.479, pp.640–650, 2019.
[20] L. Du, Z. Zhang, S. Tan, *et al*., "An Associated Deletion
Scheme for Multi-copy in Cloud Storage", *Proc. of the 18th
International Conference on Algorithms and Architectures for
Parallel Processing*, Guangzhou, China, pp.511–526, 2018.
[21] C. Yang, X. Chen and Y. Xiang, "Blockchain-based publicly
verifiable data deletion scheme for cloud storage", *Journal
of Network and Computer Applications*, Vol.103, pp.185–193,
2018.
[22] Y. Yu, J. Ni, W. Wu, *et al*., "Provable data possession
supporting secure data transfer for cloud storage", *Proc. of
2015 10th International Conference on Broadband and Wireless
Computing, Communication and Applications(BWCCA
2015)*, Krakow, Poland, pp.38–42, 2015.
[23] J. Ni, X. Lin, K. Zhang, *et al*., "Secure outsourced
data transfer with integrity verification in cloud storage",
Proc. of 2016 IEEE/CIC International Conference on Communications in China, Chengdu, China, pp.1–6, 2016.

[24] L. Xue, J. Ni, Y. Li, *et al*., "Provable data transfer from
provable data possession and deletion in cloud storage",
Computer Standards & Interfaces, Vol.54, pp.46–54, 2017.
[25] Y. Liu, X. Wang, Y. Cao, *et al*., "Improved provable data
transfer from provable data possession and deletion in cloud
storage", *Proc. of Conference on Intelligent Networking and
Collaborative Systems*, Bratislava, Slovakia, pp.445–452, 2018.