A NEW COUNTING BLOOM FILTER-BASED SCHEME, WHICH CAN GET PUBLICLY VERIFIABLE DATA DELETION

G Latha Pragathi, M. Tech, CSE, KIET-W, Kakinada

ABSTRACT:

With the fast improvement 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 difficulty, we construct a new counting Bloom filter-based scheme in this. 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.

KEYWORDS: cloud service providers, trusted third party

1] 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

Copyright @ 2021 Authors

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. For eseeably, the outsourced data transfer will become a fundamental requirement from the data owners' point of view.

2] LITERATURE SURVEY:

2.1] we propose a remote data integrity auditing scheme that realizes data sharing with sensitive information hiding in this paper. In this scheme, a sanitizer is used to sanitize the data blocks corresponding to the sensitive information of the file and transforms these data blocks' signatures into valid ones for the sanitized file. These signatures are used to verify the integrity of the sanitized file in the phase of integrity auditing. As a result, our scheme makes the file stored in the cloud able to be shared and used by others on the condition that the sensitive information is hidden, while the remote data integrity auditing is still able to be efficiently executed. Meanwhile, the proposed scheme is based on identity-based cryptography, which simplifies the complicated certificate management.

2.2] We propose a framework for privacy-preserving outsourced classification in cloud computing (POCC). Using POCC, an evaluator can securely train a classification model over the data encrypted with *different public keys*, which are outsourced from the multiple data providers. We prove that our scheme is secure in the *semi-honest* model

3] PROBLEM DEFINTION:

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.

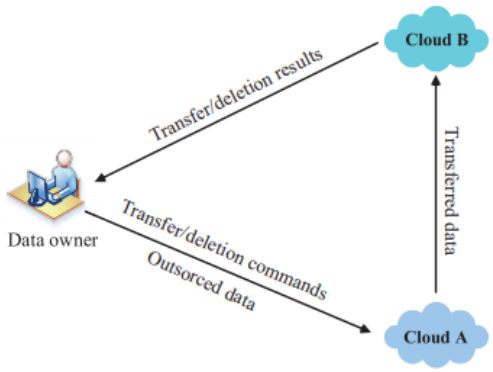
4] PROPOSED APPROACH:

We aim to achieve verifiable data transfer between two different clouds and reliable data

Copyright @ 2021 Authors

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.

5] SYSTEM ARCHITECTURE:



6] PROPOSED METHODOLOGY:

Data Owner

In this application the owner should register with the application and the owner should authorized by the admin, then the owner can able to login into his homepage. After his/her successful login data owner can able to perform some operations such as Outsourcedata, view data, Transfer Request, Deletion Request, View Results and at last logout.

Cloud_A

Here the cloudA can directly login with the application with their credentials. After cloudA successfully login he can perform view transfer request and view deletions request and at last cloudA logout.

Cloud_B

Here the cloudB can directly login with the application with their credentials. After cloudB successfully login he can perform view transfer request and view deletions request and at last cloudB logout.

Admin

Here admin also should login with the application and after his successful login admin can perform some actions such as view owner details and authorize them, view all file uploaded in cloud, view timestamp of uploading files.

7] ALGORITHM:

Copyright @ 2021 Authors

Counting Bloom filter

1. Initialization

Generate public private key pairs for the data owner, the cloud A and the cloud B, respectively.

2. Data encryption

To protect the data confidentiality, the data owner uses secure encryption algorithm to encrypt the outsourced file before uploading.

3. Data outsourcing

The cloud A stores outsource data and generates storage proof. Then the data owner checks the storage result and deletes the local backup.

4. Data transfer

When the data owner wants to change the service provider, he migrates some data blocks, even the whole file from the cloud A to the cloud B.

5. Transfer check

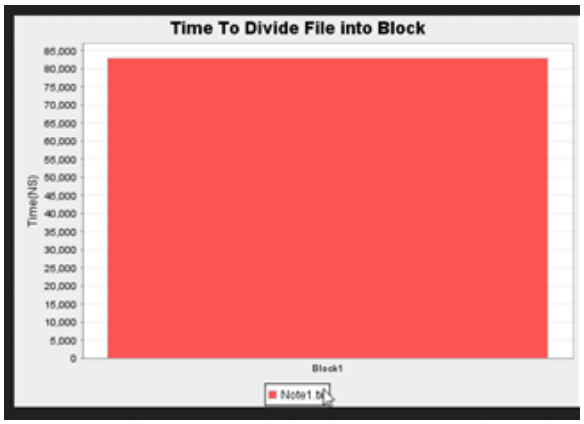
The cloud B wants to check the correctness of the transfer and returns the transfer result to the data owner.

6. Data deletion

The data owner might require the cloud A to delete some data blocks when they have been transferred to the cloud B successfully

8] RESULTS:

File Transfer Details



Time stamp in graph

9] CONCLUSION:

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

Copyright @ 2021 Authors

cloud A cannot behave maliciously and cheat the data owner successfully.

10] 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

Copyright @ 2021 Authors

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.

G Latha Pragathi, B.Tech, CSE, SRKR Engineering college, Bhimavaram., MTech, CSE, KIET-W, Kakinada. Her area of interest includes Secure Computing, Cloud Computing.

Copyright @ 2021 Authors