ISSN: 0972-2750
Vol-12 Issue-11 No.01: 2022

SECURE DATA TRANSFER AND DELETION USING COUNTER BLOOMING FILTER BY CLOUD COMPUTING

[1]Faziya, [2]S Sateesh Reddy
[1]Mtech, Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur, Karimnagar, Telangana, INDIA, H.no: 20S41D5809, fazeeya510@gmail.com
[2]Department of Computer Science, VAAGESWARI COLLEGE OF ENGINEERING Thimmapur, Karimnagar, Telangana, INDIA, sateesh.singireddy@gmail.com

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.

Keywords *– Cloud storage, Data deletion, Data transfer, Counting Bloom filter, Public verifiability*

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 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.

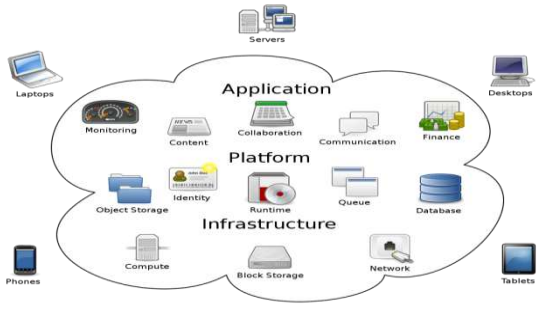


Fig.1: Example figure

ISSN: 0972-2750
Vol-12 Issue-11 No.01: 2022

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.

2. LITERATURE REVIEW

Secure and efficient fine-grained data access control scheme in cloud computing:

By combining cloud computing and Peer-to-Peer computing, a P2P storage cloud can be formed to offer highly available storage services, lowering the economic cost by exploiting the storage space of participating users. However, since cloud severs and users are usually outside the trusted domain of data owners, P2P storage cloud brings forth new challenges for data security and access control when data owners store sensitive data for sharing in the trusted domain. Moreover, there are no mechanisms for access control in P2P storage cloud. To address this issue, we design a ciphertext-policy attribute-based encryption (ABE) scheme and a proxy re-encryption scheme. Based on them, we further propose a secure, efficient and fine-grained data Access Control mechanism for P2P storage Cloud named ACPC. We enforce access policies based on user attributes, and integrate P2P reputation system in ACPC. ACPC enables data owners to delegate most of the laborious user revocation tasks to cloud servers and reputable system peers. Our security analysis demonstrates that ACPC is provably secure. The performance evaluation shows that ACPC is highly efficient under practical settings, and it significantly reduces the computation overheads brought to data owners and cloud servers during user revocation, compared with other state-of-the-art revocable ABE schemes.

New algorithms for secure outsourcing of modular exponentiations

With the rapid development of cloud services, the techniques for securely outsourcing the prohibitively expensive computations to untrusted servers are getting more and more attention in the scientific community. Exponentiations modulo a large prime have been considered the most expensive operations in discrete-logarithm-based cryptographic protocols, and they may be burdensome for the resource-limited devices such as RFID tags or smartcards. Therefore, it is important to present an efficient method to securely outsource such operations to (untrusted) cloud servers. In this paper, we propose a new secure outsourcing algorithm for (variable-exponent, variable-base) exponentiation modulo a prime in the two untrusted program model. Compared with the state-of-the-art algorithm, the proposed algorithm is superior in both efficiency and checkability. Based on this algorithm, we show how to achieve outsource-secure Cramer-Shoup encryptions and Schnorr signatures. We then propose the first efficient outsource-secure algorithm for simultaneous modular exponentiations. Finally, we provide the experimental evaluation that demonstrates the efficiency and effectiveness of the proposed outsourcing algorithms and schemes.

Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage

With cloud storage services, users can remotely store their data to the cloud and realize the data sharing with others. Remote data integrity auditing is proposed to guarantee the integrity of the data stored in the cloud. In some common cloud storage systems such as the electronic health records system, the cloud file might contain some sensitive information. The sensitive information should not be exposed to others when the cloud file is shared. Encrypting the whole shared file can realize the sensitive information hiding, but will make this shared

ISSN: 0972-2750
Vol-12 Issue-11 No.01: 2022

file unable to be used by others. How to realize data sharing with sensitive information hiding in remote data integrity auditing still has not been explored up to now. In order to address this problem, 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. The security analysis and the performance evaluation show that the proposed scheme is secure and efficient.

New provable data transfer from provable data possession and deletion for secure cloud storage

With the continuous and rapid development of cloud computing, it becomes more popular for users to outsource large-scale data files to cloud servers for storage and computation. However, data outsourcing brings convenience to users while it also causes certain security problems. The integrity of outsourced data needs to be periodically checked by users to protect their data. Also, the secure transfer of cloud data can avoid data losses to users. Aiming at solving these problems in the data outsourcing process, a provable data transfer scheme based on provable data possession and deletion is recently proposed by Xue et al. However, we found a security flaw in Xue et al.'s scheme. Concretely, the block tags can be forged in their scheme. In this article, we first give a brief review of Xue et al.'s scheme and then a detailed attack is shown. To remove the security flaw, an improved scheme is proposed. Furthermore, we replace the integrity checking protocol of their proposal with a more efficient protocol to improve the efficiency of data integrity auditing.

Data integrity checking with reliable data transfer for secure cloud storage

Currently, an increasing number of data owners prefer to store their data on remote servers due to a number of appealing advantages of cloud storage, say convenience and simplicity, scalability of the service and ubiquitous network access. However, outsourced data's transfer becomes a critical requirement for cloud users because of the emergence of various cloud storage services with different qualities of services. Therefore, the users might not only be anxious about the status of their data on cloud servers but also care whether the data are transferred entirely to the new cloud without corruption and whether the data on original cloud are discarded. To address these challenging issues, in this paper, we propose a novel auditing scheme for cloud storage services characterised by secure data transfer, provable data erasure, high error detection probability, confidential data storage. The proposed scheme can guarantee the integrity of remote data when the data are hosted on cloud servers and are transferred between two clouds, and secure deletion of the transferred data on the original cloud.

3. METHODOLOGY

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.

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

ISSN: 0972-2750
Vol-12 Issue-11 No.01: 2022

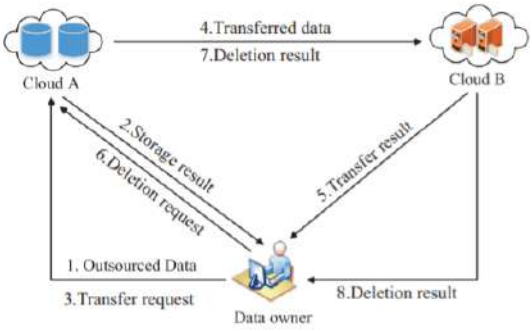
the cloud B, or delete some data from the storage medium. The cloud A and cloud B provide the data owner with cloud storage service. We assume that the cloud A is the original cloud, which will be required to migrate some data to the target cloud B, and remove the transferred data. However, the cloud 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.

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.



4. IMPLEMENTATION

The major modules of the project are

- Owner
- Admin
- ✓ Cloud(A)
- ✓ Cloud(B)

5. EXPERIMENTAL RESULTS

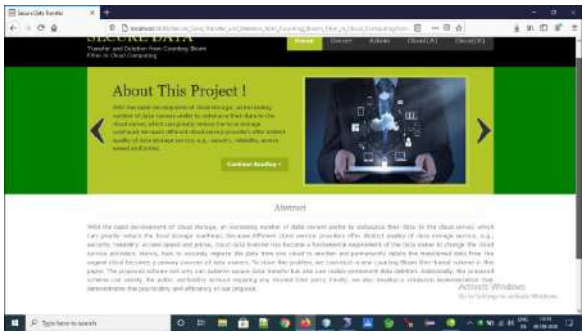


Fig.3: Home screen

ISSN: 0972-2750
Vol-12 Issue-11 No.01: 2022

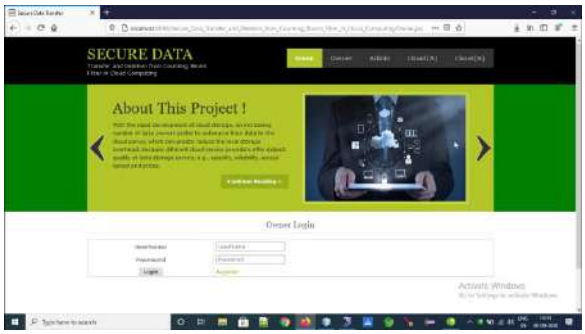


Fig.4: owner login


Fig.5: Divide data into blocks


Fig.6: Upload status

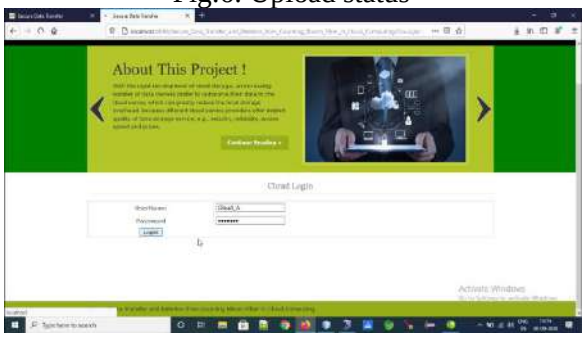


Fig.7: Cloud login

ISSN: 0972-2750
Vol-12 Issue-11 No.01: 2022

Fig.8: View transfer request

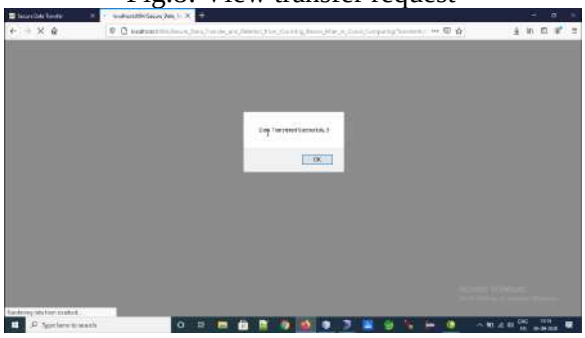


Fig.9: Data transfer status

Fig.10: Deletion status

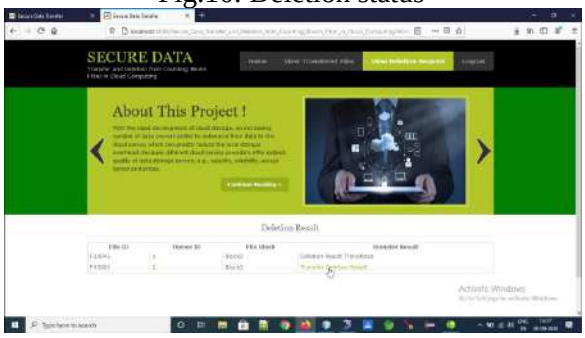


Fig.11: Deletion result

ISSN: 0972-2750
Vol-12 Issue-11 No.01: 2022

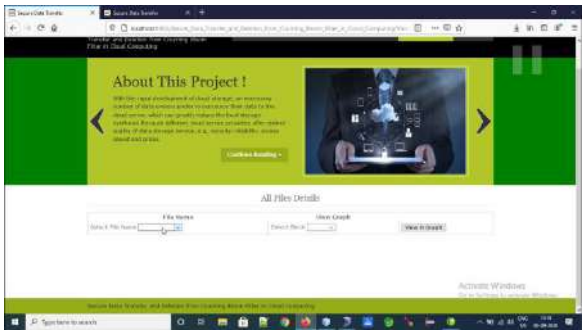


Fig.12: View time stamp

Fig.13: Time stamp in graph

6. 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 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.

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.