Secure Data Transfer and Deletion from Counting Bloom Filter in Cloud Computing.

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.

**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.

**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.

**SYSTEM REQUIREMENTS**

➢ **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