Efficient Audit Service Outsourcing
For Data Integrity in Clouds

ABSTRACT

Cloud-based outsourced storage relieves the client’s burden for storage management and maintenance by providing a comparably low-cost, scalable, location-independent platform. However, the fact that clients no longer have physical possession of data indicates that they are facing a potentially formidable risk for missing or corrupted data. To avoid the security risks, audit services are critical to ensure the integrity and availability of outsourced data and to achieve digital forensics and credibility on cloud computing. Provable data possession (PDP), which is a cryptographic technique for verifying the integrity of data without retrieving it at an untrusted server, can be used to realize audit services. Here, profiting from the interactive zero-knowledge proof system, we address the construction of an interactive PDP protocol to prevent the fraudulence of prover (soundness property) and the leakage of verified data (zero-knowledge property). We prove that our construction holds these properties based on the computation Diffie–Hellman assumption and the rewindable black-box knowledge extractor. We also propose an efficient mechanism with respect to probabilistic queries and periodic verification to reduce the audit costs per verification and implement abnormal detection timely. In addition, we present an efficient method for selecting an optimal parameter value to minimize computational overheads of cloud audit services. Our experimental results demonstrate the effectiveness of our approach.

Existing System

1) Traditional cryptographic technologies for data integrity and availability, based on hash functions and signature schemes cannot work on the outsourced data without a local copy of data.

2) In addition, it is not a practical solution for data validation by downloading them due to the expensive transaction, especially for large-size files. Moreover, the solutions to audit the correctness of the data in a cloud environment can be formidable and expensive for the cloud users.

Therefore, it is crucial to realize public auditability for CSS, so that data owners may resort to a third party auditor (TPA), who has expertise
and capabilities that a common user does not have, for periodically auditing the outsourced data. This audit service is significantly important for digital forensics and data assurance in clouds.

**PROPOSED SYSTEM**

Major concern addressed here is how to improve the performance of audit services. The audit performance concerns not only the costs of computation, communication, storage for audit activities but also the scheduling of audit activities. No doubt improper scheduling, more or less frequent, causes poor audit performance, but an efficient scheduling can help provide a better quality of and a more cost-effective service. Hence, it is critical to investigate an efficient schedule for cloud audit services.

1) How to design an efficient architecture of audit system to reduce the storage and network overheads and enhance the security of audit activities;
2) How to optimize parameters of audit systems to minimize the computation overheads of audit services.

**Algorithm Used**

Cryptographic interactive audit scheme

**Modules:**

1) Data owner (DO):

   who has a large amount of data to be stored in the cloud; data owner uses the secret key sk to preprocesses the file, which consists of a collection of n blocks, generates a set of public verification information that is stored in TPA, transmits the file and some verification tags to CSP, and may delete its local copy;

2) Cloud service provider (CSP):

   who provides data storage service and has enough storage spaces and computation resources; the data owner and granted clients need to dynamically interact with CSP to access or update their data for various application purposes.
However, we neither assume that CSP is trust to guarantee the security of stored data, nor assume that the data owner has the ability to collect the evidences of CSP’s fault after errors occur.

3) Third party auditor (TPA):
   TPA, Who has capabilities to manage or monitor outsourced data under the delegation of data owner; TPA, as a trust third party (TTP), is used to ensure the storage security of their outsourced data. We assume the TPA is reliable and independent, and thus has no incentive to collude with either the CSP or the clients during the auditing process:

4) Granted applications (GA):
   who have the right to access and manipulate stored data. These applications can be either inside clouds or outside clouds according to the specific requirements.

5) Cryptographic interactive audit scheme:
   We prove that this scheme retains the soundness property and zero-knowledge property of proof systems. These two properties ensure that our scheme can not only prevent the deception and forgery of cloud storage providers, but also prevent the leakage of outsourced data in the periodic verification for improving performance of audit services. To detect abnormal situations timely, we adopt a way of sampling verification at appropriate planned intervals.

System Requirements:

Hardware Requirements:

• System : Pentium IV 2.4 GHz.
• Hard Disk : 40 GB.
• Floppy Drive : 1.44 Mb.
• Monitor : 15 VGA Colour.
• Mouse : Logitech.
• Ram : 512 Mb.
S/W System Configuration:-

- Application Server: Tomcat6.0.18
- Front End: HTML, Java, Jsp
- Scripts: JavaScript.
- Server side Script: Java Server Pages.
- Database: mysql 5.0
- Database Connectivity: JDBC.

Architecture