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. In this paper, 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.
Audit system architecture for cloud computing
Existing System

To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met:

1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user

2) The third party auditing process should bring in no new vulnerabilities towards user data privacy.

Proposed System

In this paper, we utilize the public 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. It with random mask technique to achieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind.

To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient. We also show how to extent our main scheme to support batch auditing for TPA upon delegations from multi-users.
Modules

1. Audit Service System
2. Data Storage Service System
3. Audit Outsourcing Service System
4. Secure and Performance Analysis

Audit Service System

In this module we provide an efficient and secure cryptographic interactive audit scheme for public audit ability. We provide an efficient and secure cryptographic interactive 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 process of verification.

Data Storage Service System

In this module, we considered FOUR entities to store the data in secure manner:

1. Data owner (DO)
   Who has a large amount of data to be stored in the cloud.
2. Cloud service provider (CSP)
   Who provides data storage service and has enough storage spaces and computation resources.
3. Third party auditor (TPA)
   Who has capabilities to manage or monitor – outsourced data under the delegation of data owner.
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.
Audit Outsourcing Service System

In this module the client (data owner) uses the secret key to preprocess the file, which consists of a collection of blocks, generates a set of public verification information that is stored in TPA, transmits the file and some verification tags to Cloud service provider CSP, and may delete its local copy.

At a later time, using a protocol of proof of retrievability, TPA (as an audit agent of clients) issues a challenge to audit (or check) the integrity and availability of the outsourced data in terms of the public verification information. It is necessary to give an alarm for abnormal events.

Secure and Performance Analysis

In this module, we considered to secure the data and give performance to the following:

- Audit-without-downloading
  To allow TPA (or other clients with the help of TPA) to verify the correctness of cloud data on demand without retrieving a copy of whole data or introducing additional on-line burden to the cloud users.

- Verification-correctness
  To ensure there exists no cheating CSP that can pass the audit from TPA without indeed storing users’ data intact.

- Privacy-preserving
  To ensure that there exists no way for TPA to derive users’ data from the information collected during the auditing process.

- High-performance
  To allow TPA to perform auditing with minimum overheads in storage, communication and computation, and to support statistical audit sampling and optimized audit schedule with a long enough period of time.
Hardware Required:

System : Pentium IV 2.4 GHz
Hard Disk : 40 GB
Floppy Drive : 1.44 MB
Monitor : 15 VGA color
Mouse : Logitech.
Keyboard : 110 keys enhanced
RAM : 256 MB

Software Required:

O/S : Windows XP.
Language : Asp.Net, c#.