**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 serv er, can be used to realize audit services. In this paper, pro fiting f rom 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 rewind able 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.

Architecture:

Literature Survey

1. **Towards Achieving Accountability, Auditability and Trust in Cloud Computing**

The lack of confidence in entrusting sensitive information to cloud computing service providers (CSPs) is one of the primary obstacles to widespread adoption of cloud computing, as reported by a number of surveys. From the CSPs’ perspective, their long-term return-on-investment in cloud infrastructure hinges on overcoming this obstacle. Encryption and privacy protection techniques only solve part of this problem: in addition, research is needed to increase the accountability and auditability of CSPs. However, achieving cloud accountability is a complex challenge; as we now have to consider large-scale virtual and physical distributed server environments to achieve (1) real-time tracing of source and duplicate file locations, (2) logging of a file’s life cycle, and (3) logging of content modification and access history. This position paper considers related research challenges and lays a foundation towards addressing these via three main abstraction layers of cloud accountability and a Cloud Accountability Life Cycle.

**2. Scalable and Efficient Provable Data Possession**

Storage outsourcing is a rising trend which prompts a number of interesting security issues, many of which have been extensively investigated in the past. However, Provable Data Possession (PDP) is a topic that has onlyrecently appeared in the research literature. The main issue is how to frequently, efficiently and securely verify that a storage server is faithfully storing its client’s (potentially very large) outsourced data. The storage server is assumed to be untrusted in terms of both security and reliability. (In other words, it might maliciously or accidentally erase hosted data; it might also relegate it to slow or off-line storage.) The problem is exacerbated by the client being a small computing device with limited resources. Prior work has addressed this problem using either public key cryptography or requiring the client to outsource its data in encrypted form. In this paper, we construct a highly efficient and provably secure PDP technique based entirely on symmetric key cryptography, while not requiring any bulk encryption. Also, in contrast with its predecessors, our PDP technique allows outsourcing of dynamic data, i.e, it efficiently supports operations, such as block modification, deletion and append.

**3. Dynamic Provable Data Possession**

As storage-outsourcing services and resource-sharing networks have become popular, the problem of efficiently proving the integrity of data stored at untrusted servers has received increased attention.In the provable data possession (PDP) model, the client preprocesses the data and then sends it to an untrusted server for storage, while keeping a small amount of meta-data. The client later asks the server to prove that the stored data has not been tampered with or deleted (without downloading the actual data). However, the original PDP scheme applies only to static (or append-only) files. We present a definitional framework and efficient constructions for dynamic provable data possession (DPDP), which extends the PDP model to support provable updates to stored data. We use a new version of authenticated dictionaries based on rank information. The price of dynamic updates is a performance change from O(1) to O(log n) (or O(nǫ log n)), for a file consisting of n blocks, while maintaining the same (or better, respectively) probability of misbehavior detection. Our experiments show that this slowdown is very low in practice (e.g., 415KB proof size and 30ms computational overhead for a 1GB file). We also show how to apply our DPDP scheme to outsourced file systems and version controlsystems(e.g.,CVS).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

2) The third party auditing process should brin g in no new vulnerabilities

**Proposed System**

In this paper, we utilize the public provable data possession 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 retrieving it at an untrusted server; can be used to realize audit services. publicauditingcloud 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 aggr egate signature to extend our main result into a multi- user setting, where TPA can perform multiple auditing tasks simultaneously.user setting, where TPA can perform multiple auditing tasks simultaneously.Ex tensive security and performance analysis shows the proposed schemes areprovably secure and highly efficient. We also show how to extent our main scheme tosupport batch auditing fo r 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. Th ese two properties ensure that our scheme can not only prevent the deception and forger y of cloud storage providers, but also prevent the leakage of outsourced data in the p rocess of verification.

**Data Storage Service System**

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

**Data owner (DO)**

Who has a large amount of data to be stored in the cloud

**Cloud service provider (CSP)**

Who provides data storage service and has enou gh 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 abno rmal 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.

**SYSTEM SPECIFICATION**

**Hardware Requirements**

System : Pentium IV 2.4 GHz.

Hard Disk : 40 GB

Floppy Drive : 1.44 Mb

Monitor : 14’ Colour Monitor

Mouse : Optical Mouse

Ram : 512 Mb

Keyboard : 101 Keyboard.

**Software Requirements**

 Operating system : Windows XP

 Coding Language : ASP.Net with C#

 Data Base : SQL Server 2005