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

**OBJECTIVE:**

We propose a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud.

**DOMAIN:** Cloud computing

**SYNOPSIS:**

In this paper, we propose a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud. In particular, we exploit ring signatures to compute verification metadata needed to audit the correctness of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private from public verifiers, who are able to efficiently verify shared data integrity without retrieving the entire file. In addition, our mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one.

The propose system Oruta, a privacy-preserving public auditing mechanism for shared data in the cloud. We utilize ring signatures to construct homomorphism authenticators, so that a public verifier is able to audit shared data integrity without retrieving the entire data, yet it cannot distinguish who is the signer on each block. To improve the efficiency of verifying multiple auditing tasks, we further extend our mechanism to support batch auditing. There are two interesting problems we will continue to study for our future work. One of them is traceability, which means the ability for the group manager to reveal the identity of the signer based on verification metadata in some special situations

**EXISTING SYSTEM:**

The existing mechanism a new significant privacy issue introduced in the case of shared data with the use of the leakage of identity privacy to public verifiers. The traditional approach for checking data correctness is to retrieve the entire data from the cloud, and then verify data symmetric keys by checking the correctness of signatures.

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

**LIMITATIONS**

* As users no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted.
* They do not perform the multiple auditing task in simultaneously.

**PROPOSED SYSTEM:**

The propose system Oruta, a privacy-preserving public auditing mechanism for shared data in the cloud. We utilize ring signatures to construct homomorphism authenticators, so that a public verifier is able to audit shared data integrity without retrieving the entire data, yet it cannot distinguish who is the signer on each block.

To improve the efficiency of verifying multiple auditing tasks, we further extend our mechanism to support batch auditing. There are two interesting problems we will continue to study for our future work. One of them is traceability, which means the ability for the group manager to reveal the identity of the signer based on verification metadata in some special situations

**ADVANTAGES:**

* The proposed system can perform multiple auditing tasks simultaneously
* They improve the efficiency of verification for multiple auditing tasks.
* High security provide for file sharing.

**SYSTEM ARCHITECTURE**

Third party auditor

Security message flow

Auditing challenges

EmailAuditing

Proofs

Cloud Server

**Upload/download**

Users

Share Data Flow

Security message flow

**HARDWARE AND SOFTWARE SPECIFICATION:**

**Software Requirement:**

1. Language - Java(JDK 1.7)
2. OS - Windows 7 32bit
3. MySql Server
4. NetBeans IDE 7.1.2

**Hardware Requirement :**

1. 1 GB RAM
2. 80 GB Hard Disk
3. Above 2GHz Processor
4. Data Card