NPP A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users

ABSTRACT

The increasing number of applications of shared data, such as iCloud, Google Docs, and so on, users can upload their data to a cloud and share it with other peers as a group. Unfortunately, since cloud servers are vulnerable to inevitable hardware faults, software failures or human errors, data stored in the cloud may be spoiled or lost [1]. In the worst cases, a cloud owner may even conceal data error accidents in order to preserve its reputation or avoid profit losses [2],[3]. In addition, users who lose direct control over their data are not sure whether their cloud-stored data is intact or not. Therefore, integrity verification for the shared data in the cloud is an important, yet timely issue for a large number of cloud users.

EXISTING SYSTEM

To ensure the integrity of data stored in cloud servers, a number of mechanisms based on various techniques have been proposed. In particular, in order to reduce the burden on users, a trusted third-party auditor (TPA) is engaged to conduct the verification, which is called public auditing [4]. However, the TPA may have unnecessary access to private information during the auditing process [5]. Therefore, researchers proposed some new schemes to protect privacy, including data privacy [6], and identity privacy [7]-[9]. To be specific, the TPA cannot learn each block that is signed by a particular user in the group by constructing homomorphic authenticable ring signatures [7] or computing tags based on common group private key [8]. However, since both methods concern about unconditional privacy, the real identity of the signer can no longer be traced. A later development is the homomorphic authenticable group signature scheme based on group signatures [9], which is designed to protect privacy. On one hand, the identity of each signer is anonymous; and on the other hand, the group manager can trace a signer's real identity after a dispute. Unfortunately, in all existing public auditing schemes, the tracing process is accomplished by a single entity. As a result, that entity has the privilege of tracing, which may lead to abuse of single authority power. Therefore, an innocent user may be framed or a malicious user may be harbored.

DRAWBACKS

- Ring signatures & computing tags based on common group private key both methods concern about unconditional privacy, the real identity of the signer can no longer be traced.
- Entity has the privilege of tracing, which may lead to abuse of single authority power. May Leads to an innocent user may be framed or a malicious user may be harbored.

PROPOSED SYSTEM

We propose a new privacy-aware public auditing mechanism for shared cloud data by constructing a homomorphic verifiable group signature. Unlike the existing solutions, our scheme requires at least *t* group managers to recover a trace key cooperatively, which eliminates the abuse of single-authority power and provides non-frameability. Moreover, our scheme ensures that group users can trace data changes through designated binary tree; and can recover the latest correct data block when the current data block is damaged. In addition, the formal security analysis and experimental results indicate that our scheme is provably secure and efficient.

ADVANTAGES

- Proposed scheme can not only provide multi-levels privacy-preservation abilities, but also can well support group user revocation.

- We design a data structure based on a binary tree for clouds to record all the changes of data blocks. Group users can trace the data changes through the binary tree and recover the latest correct data block when the current data block is damaged.

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

- **S/W System Configuration:-**
- Operating System : Windows 7 or 8 32 bit
- Application Server : Tomcat5.0/6.X
- Backend coding : Java
- Tool : Virtual Box

- Environment : Ubuntu
- Technology : Hadoop