

NPP A new privacy –Aware public Auditing scheme for Cloud storage data sharing with group users

Abstract:

Due to 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.

Existing system:

In the existing system a privacy-preserving public auditing scheme, called *Oruta*, for shared data in the cloud. Their scheme was based on a homomorphic authenticable ring signature, which allows a public auditor to audit the shared data without retrieving all data from the cloud. However, the auditing overhead linearly increases with the number of group users; hence it is not suitable for large groups in the cloud. To support large groups, Wang *et al.* proposed a new auditing scheme, called *Knox*. The auditing overhead is independent of the number of group users, hence *Knox* can support shared data with large groups. Moreover, any group manager can reveal the identity of the signer. Unfortunately, the scheme cannot support user revocation.

Disadvantages:

1. Security levels are low in the existing systems.
2. Users revocations are not possible.

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 nonframeability. Moreover, our scheme ensures

Further Details Contact: A Vinay 9030333433, 08772261612, 9014123891

#301, 303 & 304, 3rd Floor, AVR Buildings, Opp to SV Music College, Balaji Colony, Tirupati - 515702

Email: info@takeoffprojects.com | www.takeoffprojects.com

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.

Advantages:

1. Security levels have been improved compare to existing systems.
2. Data recovery and data can be traced out which data block is getting damaged.
3. Suspected users revocation can be performed.

SYSTEM REQUIREMENTS

H/W System Configuration:-

- Processor - Pentium –III
- RAM - 256 MB (min)
- Hard Disk - 20 GB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA

S/W System Configuration:-

- Operating System : Windows95/98/2000/XP
- Application Server : Tomcat5.0/6.X
- Front End : HTML, Jsp
- Scripts : JavaScript.
- Server side Script : Java Server Pages.
- Database : MySQL 5.0
- Database Connectivity : JDBC