Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud

Abstract:

With data storage and sharing services in the cloud, users can easily modify and share data as a group. To ensure shared data integrity can be verified publicly, users in the group need to compute signatures on all the blocks in shared data. Different blocks in shared data are generally signed by different users due to data modifications performed by different users. For security reasons, once a user is revoked from the group, the blocks which were previously signed by this revoked user must be re-signed by an existing user. The straightforward method, which allows an existing user to download the corresponding part of shared data and re-sign it during user revocation, is inefficient due to the large size of shared data in the cloud. In this paper, we propose a novel public auditing mechanism for the integrity of shared data with efficient user revocation in mind. By utilizing the idea of proxy re-signatures, we allow the cloud to re-sign blocks on behalf of existing users during user revocation, so that existing users do not need to download and re-sign blocks by themselves. In addition, a public verifier is always able to audit the integrity of shared data without retrieving the entire data from the cloud, even if some part of shared data has been re-signed by the cloud. Moreover, our mechanism is able to support batch auditing by verifying multiple auditing tasks simultaneously. Experimental results show that our mechanism can significantly improve the efficiency of user revocation.

Existing System:

In existing system a signature block is attached to each block in data and the integrity of data relies on the correctness of all the signatures. One of the most significant and common features of these mechanisms is to allow public verifier to efficiently check the data integrity in the cloud without downloading the entire data, referred to as public auditing. This public verifier could be client who would like to utilize the cloud data for particular purposes or a thirdparty auditor who is able to provide verification services on data integrity to users. With shared data, once a user modifies a block he also need to compute a new signature for the modified block. Due to modifications from different users different blocks are signed by different users. For security reasons when a user leaves or misbehaves this user must
be revoked from the group. As a result, this revoked user is no longer able to share and modify the data, and the signatures generated by this revoked user are no longer valid to the group.

**Disadvantages:**

1. Straightforward method may cost the existing user huge amounts of communication and computation resources.

2. The number of resigned block is quite large or the membership of the group is frequently changing.

**Proposed System:**

In this paper, we propose PANDA a novel public auditing mechanism for the integrity of shared data with efficient user revocation in the cloud. In our mechanism by utilizing the idea of proxy re-signatures, once a user in the group is revoked, the cloud is able to resign the blocks signed by the revoked user using a resigning key. As a result, the efficiency of user revocation can be significantly improved.

**Advantages:**

1. It follows protocol and does not pollute data integrity actively as a malicious adversary.

2. Cloud data can be efficiently shared among a large number of users, and the public verifier is able to handle the large number of auditing tasks simultaneously and efficiently.
System Requirements:

Hardware Requirements:

- System: Pentium IV 2.4 GHz.
- Hard Disk: 40 GB.
- Floppy Drive: 1.44 Mb.
- Monitor: 15 VGA Colour.
- Mouse: Logitech.
- Ram: 512 Mb.

Software Requirements:

- Coding Language: C#, Asp.net
- IDE: VisualStudio 2010