Overt Auditing for Mutual Data with High Octane User Repeal in the Cloud

S. Malini
Assistant Professor
Department of Computer Science & Engineering
C.Abdul Hakeem College of Engineering & Technology, Melvisharam, Tamilnadu, India

B. Pavithra
Assistant Professor
Department of Computer Science & Engineering
C.Abdul Hakeem College of Engineering & Technology, Melvisharam, Tamilnadu, India

N. Nazeema
Assistant Professor
Department of Computer Science & Engineering
C.Abdul Hakeem College of Engineering & Technology, Melvisharam, Tamilnadu, India

Abstract

With data storage and sharing services in the cloud, users can easily modify and share data as a group. To ensure share 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 tore-sign blocks on behalf of existing users during user revocation, so that existing users do not need to download and re-sign blocks. In addition, a public verifier is always able to audit the integrity of shared data without retrieving the entire data from the Cloud. Moreover, our mechanism is able to support batch auditing by verifying multiple auditing tasks simultaneously, results show that our mechanism can significantly improve the efficiency of user revocation.

Keywords: User revocation, re-signatures, PANDA, re-signing proxies, public verifier,public auditor

I. INTRODUCTION

A. Aim of Project:

With data storage and sharing services (such as Drop box and Google Drive) provided by the cloud, people can easily work together as a group by sharing data with each other, we propose a proxy re-signature.

B. Over View of Project:

More specifically, once a user creates shared data in the cloud, every user in the group is able to not only access and modify shared data, but also share the latest version of the shared data with the rest of the group. Although cloud providers promise a more secure and reliable environment to the users, the integrity of data in the cloud may still be compromised, due to the existence of hardware/software failures and human errors.

To protect the integrity of data in the cloud, a number of mechanisms have been proposed. In these mechanisms, a signature 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 a public verifier to efficiently check data integrity in the cloud without downloading the entire data, referred to as public auditing (or denoted as Provable Data Possession. This public verifier could be a client who would like to utilize cloud data for particular purposes(e.g., search, computation, data mining, etc.) or a third party auditor (TPA) who is able to provide verification services on data integrity to users. Most of the previous works focus on auditing the integrity of personal data.

Different from these works, several recent works focus on how to preserve identity privacy from public verifiers when auditing the integrity of shared data. Unfortunately, none of the above mechanisms, considers the efficiency of user revocation when auditing the correctness of shared data in the cloud. With shared data, once a user modifies a block, she also needs to compute a new signature for the modified block.

II. EXISTING SYSTEM

A. System Description:

An existing system the file uploaded in cloud which not signed by user in each time of upload. So that integrity of shared data is not possible in existing system. However, since the cloud is not in the same trusted domain with each user in the group, outsourcing every user's private key to the cloud would introduce significant security issue.

B. Drawbacks of Existing System:

Straightforward method may cost the existing user a huge amount of communication and computation resources .The number of re-signed blocks is quite large or the membership of the group is frequently changing.

III. PROPOSED SYSTEM

A. System Description:

In our Proposed system may lie to verifiers about the incorrectness of shared data in order to save the reputation of its data services and avoid losing money on its data services. In addition, we also assume there is no collusion between the cloud and any user during the design of our mechanism. Generally, the incorrectness of share data under the above semi trusted model can be introduced by hardware/software failures or human errors happened in the cloud. Considering these factors, users do not fully trust the cloud with the integrity of shared data.

B. Advantages of Proposed System :

Multiple re-signing proxies ,Login with secret key in each time.Efficiency of user revocation can be significantly improved, Computation and communication resources of existing users can be easily saved .

IV. SYSTEM ARCHITECTURE

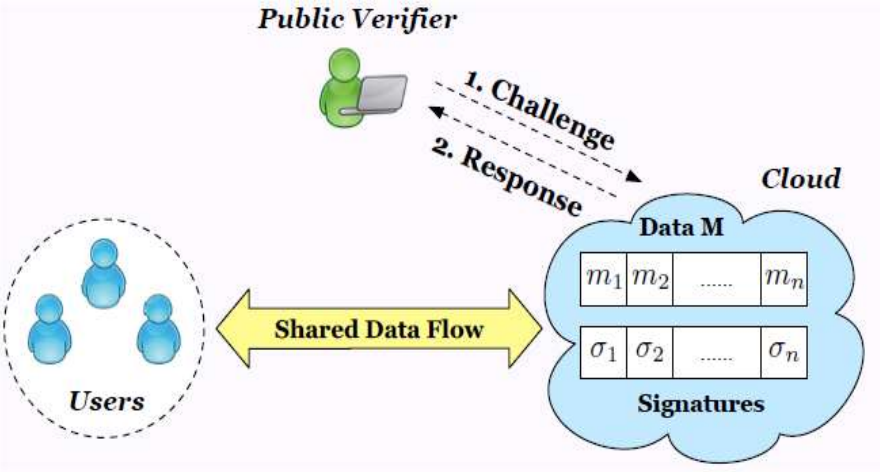

Fig. 4.1: Architecture Diagram

V. USER MODULE

A. Registration:

In this module each user register his user details for using files. Only registered user can able to login in cloud sever

B. File Upload:

In this module user upload a block of files in the cloud with encryption by using his secret key. This ensures the files to be protected from unauthorized user.

C. Download:

This module allows the user to download the file using his secret key to decrypt the downloaded data of blocked user and verify the data and re-upload the block of file into cloud server with encryption .This ensure the files to be protected from unauthorized user.

D. Re-upload:

This module allow the user to re-upload the downloaded files of blocked user into cloud server with resign the files(i.e.) the files is uploaded with new signature like new secret with encryption to protected the data from unauthorized user

E. Unblock Module

This module allow the user to unblock his user account by answering his security question regarding to answer that provided by his at the time of registration. Once the answer is matched to the answer of registration time answer then only account will be unlocked.

VI. AUDITOR MODULE

A. File Verification Module:

The public verifier is able to correctly check the integrity of shared data. The public verifier can audit the integrity of shared data without retrieving the entire data from the cloud, even if some blocks in shared data have been re-signed by the cloud.

B. Files View:

In this module public auditor view the all details of upload, download, blocked user, re-upload.

VII. ADMIN MODULE

A. View Files:

In this module public auditor view the all details of upload, download, blocked user, re-upload.

B. Block User:

In this module admin block the misbehave user account to protect the integrity of shared data.

VIII. CONCLUSION

In this project, we proposed a new public auditing mechanism for shared data with efficient user revocation in the cloud. When a user in the group is revoked, we allow the semi-trusted cloud to re-sign blocks that were signed by the revoked user with proxy re-signatures. Experimental results show that the cloud can improve the efficiency of user revocation, and existing users in the group can save a significant amount of computation and communication resources during user revocation.

REFERENCES

[1] [1]. Armbrust.M, Fox .A, Griffith .A, Joseph .A. D, Katz .R. H., Konwinski .A, Lee .G, Patterson .D. A., Rabkin. A, Stoica .I, and Zaharia .M,(2010) 'A View of Cloud Computing', Communications of the ACM, vol. 53, no. 4, pp. 50–58.
[2] [2]. Ateniese .G, Burns .R, Curtmola .R, Herring .J, Kissner. L, Peterson.Z, And Son. D, (2007)'Provable Data Possession at Untrusted Stores,' in the Proceedings of ACM CCS 2007, pp. 598–610.
[3] [3]. Shacham .H and Waters .B, (2008)'Compact Proofs of Retrievability,' in the Proceedings of ASIACRYPT 2008. Springer-Verla,pp.90–107.
[4] [4]. Wang .B and H. Li,(2013) 'Public Auditing for Shared Data with Efficient User Revoation in the Cloud,' in the Proceedings of IEEE INFOCOM 2013, pp. 2904–2912.
[5] [5]. Wang .C, Wang .Q, Ren.K, and Lou .W,(2009) 'Ensuring Data Storage Security in Cloud Computing,' in the Proceedings of ACM/IEEE IWQoS 2009, pp. 1–9.

