

User revocation for security in computing

Justin Sophia. I¹ and Amali Mary Bastina. A²

^{1,2}Department of Computer Science

Loyola College, Chennai 600034

¹Justinsophia4@gmail.com, ²amali.tina@yahoo.com

Abstract

In the cloud environment users can easily modify and share data as a group. Hence to ensure the broadcast data integrity is verified publicly, the users in the group need to be compute signatures on all the blocks in the broadcast data. So keeping in the mind integrity of the shared data with an efficient user revocation we propose a novel public auditing mechanism. By utilizing the idea of proxy re-signatures. We therefore allow the cloud to re-sign blocks on behalf of the existing users during user revocation, so that the existing users do not need to download and re-sign the blocks by themselves. Hence without retrieving the entire the data from the cloud always the public verifier is able to audit the integrity of the shared data . It is able to support the batch auditing by verifying the multiple auditing tasks simultaneously.

AMS Subject Classification: ...

Key Words and Phrases: Cloud Computing, broadcast data, user revocation, security.

1 Introduction

1.1 About the System

The cloud provides data storage and sharing services; people can easily work together as a group by sharing data with each other. More specifically when a user creates the shared data in the cloud,

every user in the group is able to not only access and modify the shared data. The correctness of all the signatures are based on the integrity of the data it is attached along with signature to each block in data .Therefore, it is efficiently reduce the significant burden to existing users introduced by the user revocation ,and still allow a public verifier to check the integrity of shared data without downloading. Panda is a proposed public auditing mechanism for the integrity of shared data with efficient user revocation in the cloud. It is utilizing the idea of proxy re-signatures, once a user in the group is revoked; the cloud is able to resign the blocks, which were signed by the revoked user, with an e-signing key. It is not only able to efficiently support a large number of users data and but also able to handle multiple auditing tasks simultaneously with batch auditing.

1.2 Privacy and Public Auditing Security

In privacy and public auditing security the privacy is one of the fundamental obstacles for the success of cloud computing. Privacy becomes the major concern with regard to the cloud computing. This is because the fact or information of the customers data and business logic both is stored in the distrusted cloud servers, which are owned and maintained by the cloud provider [9].

A privacy preserving policy-based content sharing in public clouds is implemented using a broadcast group key management (BGKM) scheme [5]. Redundant encryption of the same record is required to support attribute-based access control policies (acps) involving disjunctions. Another public auditing mechanism for shared data is implemented with efficient user revocation in the cloud [4]. This mechanism implements integrity of shared data with efficient user revocation in mind. By utilizing the idea of proxy re-signatures, the cloud can perform to re-signing of blocks on behalf of 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.

Yet another technique is where a source multi owner data sharing scheme is used for dynamic groups in the cloud [4].By leveraging group signature and dynamic broadcast encryption techniques, any

cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of this scheme are independent with the number of revoked users. But unfortunately it is not highly efficient in dynamics for storage security in cloud computing [7].

As the data is physically not accessible to the user, the cloud should provide a way for the user to check if the integrity of his data is maintained or is compromised. Also checking the integrity of data without downloading them, known as public auditing, is as well an efficient and effective method.

2 Techniques Used for Public Auditing

The data integrity and the cloud users computation resources as well as online burden is of importance to enable a public auditing service for the cloud data storage, so that the users may restore to an independent third-party auditor (TPA) for auditing the outsourced data whenever needed. The TPA periodically check the integrity of all the data stored in the cloud on behalf of all the users, which provides an easier and affordable ways for the users to ensure the storage correctness in the cloud. In addition to help the user to evaluate the risk of their subscribed cloud data services, the audit result from the TPA would also be beneficial for the cloud service providers to improve the cloud-based services platform, and even serve for independent arbitration purposes. Thus enabling public auditing services play an important role for this cloud economy to be fully established; where users will need ways to assess risks and gain trust in the cloud. The public audit ability has been proposed in the context of ensuring remotely stored data integrity under the different systems and security models. A brief survey of various techniques has been discussed further.

3 Classification of Cryptography

The protection methods had found their routes in cryptographic algorithms and digital signature techniques. The cryptographic algorithms are classified into two categories they are symmetric and asymmetric algorithms. The symmetric algorithms use a secret key

both for encrypting and decrypting process. The asymmetric algorithm use two keys 1) public 2) private. These public keys are used publicly whereas the private key which is kept secret used to decrypt the data. Breaking of the private is really possible even if the corresponding public key is known well in advance. The examples of symmetric algorithm and asymmetric algorithms are as following: symmetric algorithm consist of international data encryption algorithm (IDEA), advanced encryption standard (AES) the asymmetric key algorithm include RAS algorithm.

After reviewing the data security requirements the following recommendations have been included in multiparty SLA which is suggested at the end to ensure the data security in the cloud:

- The Encrypted data and the decryption key must not be stored at the same place.
- The Access control techniques are applicable for malicious insiders and privileged users.
- The independent audits must be conducted to access the effectiveness of the techniques employed for the data storage.
- The Service providers must abide to the ethics and legal laws and should be responsible for the discrepancies
- Backup and rest methods against system crash and failures.

The goal is to test whether batching is practical and, whether the benefits of removing pairings significantly outweigh the cost of the additional operations required for batching. They include the group membership testing, randomness generation, and the additional modular exponentiation and multiplications.

4 Problem Definition

The integrity of the data in cloud storage, however, is subject to the skepticism and scrutiny. As the data stored in the cloud easily be lost or corrupted due to the human errors and hardware/software failures. The traditional approach for checking the data correctness is to retrieve the entire data from the cloud. The main reason is that the size of the cloud data is large.

5 Related Work

In an existing work it is said to be download an entire resigning blocks data from the cloud. This takes much of the time and the bandwidth. For the integrity reasons we have to verify the entire resigning data downloaded from the cloud with the resigning keys.

Drawbacks:

- Maintenance Cost is high for checking all the resigning keys in the cloud.
- Security and Integrity id low.
- Require more bandwidth to download.

6 Proposed Work

To solve the existing privacy issue on the shared data, the proposed mechanisms are Panda and novel privacy Preserving public auditing technique. More specifically, we utilize the ring signatures to construct the Homomorphism authenticators and proxy re-signatures in the panda, so that a public verifier is able to verify the integrity of the shared data by not retrieving the entire data while the identity of the signer on each block in the shared data is kept private from the public verifier. In addition, the extend mechanism include in future to support batch auditing, therefore multiple auditing tasks.

The original user acts as the group manager, who is able to revoke users from the group when it is necessary, it is necessary for the cloud service providers to storage data and keys separately on different servers inside the cloud in practices.

Proposed Technique: PANDA-public auditing shared data.

Technique Definition: Panda is public auditing mechanism. It has following algorithms: Keygen, re-keygen, signgen, re-signgen, proffgen and proofver.

7 Project Description

7.1 Implementation

The implementation section is done by creating a frame work by means of web application using .net with SQL-server. Before that a data base is created which was to be processed. On which block, signature, block identifier and signer identifier were segmented which enables the user to change the single block effectively without modifying the block identifiers of other blocks.

Initially the user choose the prepared data to be processed and he creates a key generation for the group in which the data to be shared. Then the file is blocked and encrypted mean while the block segmentation is done as described above. The user in the data wants to shared by the user in the group then the cloud verifier check the validity and retrieval is done by decrypting the file the original data is viewed.

7.2 Module description

- Authentication: In this module user wants to give the database to admin all the registration process and all the process is done by admin after the registration process complete a user can get the authentication permission by using the user name / password of the website. If the user enters a valid user-name/password combination then they will be granted to access data.
- User-Registration: Every user registers his user particulars for using files. Only registered user can capable to login in cloud server.
- File Upload: User uploads a block of files in the cloud with encryption by means of his secret key. Download: This allows the user to download the file by means of his secret key to decrypt the downloaded data of blocked user and authenticate the data and re-upload the block of file into cloud server with encryption.
- Reupload: The files are uploaded with new autograph like

new secret with encryption to protect the data from not permitted user.

- Unblock: This permits the user to clear his user account by responding his safety query concerning to answer that offered by his at the time of registration.
- Admin-View Files: Public auditor outlook the all particulars of upload, download, blocked user, re upload. Block User: Admin wedge the misbehave user account to defend the honesty of shared data.

7.3 Auditor Module

- File Verification Module: The public verifier can review the truthfulness of shared data without get back the entire data from the cloud, even if some blocks in joint data have been re-signed by the cloud.
- Files View: Public auditor observation the all information of upload, download, blocked user, reupload.

7.4 Maintain revocation list

The storage in cloud gets the resignation user details from the company and maintains the revocation list because to identify the unauthorized users as they cannot access the cloud resource at any time, revoked users is incapable of using the cloud again once they are revoked.

8 Conclusion

A new public auditing mechanism for the shared data with an efficient user revocation in the cloud are been concluded when a user in the group is revoked, it allows the semi-trusted cloud to re-sign blocks that were signed by the revoked user with proxy re-signatures. Thus the cloud can improve the efficiency of user revocation, and existing users in this group can save a lot of their computation and communication resources during the user revocation.

References

- [1] Expansion embedding techniques for reversible watermarking, D.M. Thodi, J.J. Rodriguez, Senior Member, IEEE, *IEEE Transact. Image Process* (2007) **16(3)**.
- [2] Reversible data hiding, Z. Ni, Y.-Q. Shi, N. Ansari, W. Su, *IEEE Transact. Circuit. Syst. FOR Vid. Tech.* (2006) **16(3)**.
- [3] IEEE Transact. Signal Process. (2004) **52(10)**.
- [4] On compressing encrypted data, M. Johnson, student member, IEEE, P. Ishwar, V. Prabhakaran, Student Member, IEEE.
- [5] D. Schonberg, Student Member, IEEE, K. Ramachandran, senior member, IEEE.
- [6] Reversible data hiding based on multilevel histogram modification and sequential recovery
- [7] Z. Zhao, B. Hoa, Luoc,* , Zhe-Ming Luc, J.-S. Pand *Int. J. Electron. Commun. (AEU)*.
- [8] C. Wang, Q. Wang, K. Ren, W. Lou, Privacy preserving public auditing for data storage Security in Cloud Computing, In: *Proceedings of IEEE INFOCOM 2010* (2010), 525–533.
- [9] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, S.S. Yau, Dynamic audit services for integrity verification of outsourced storage in clouds, In: *Proceedings of ACM SAC 2011* (2011), 1550–1556.
- [10] C. Wang, Q. Wang, K. Ren, W. Lou, Towards secure and dependable storage services in cloud computing, *IEEE Transact. Serv. Comput.*, **5(2)** (2011), 220–232.
- [11] Y. Zhu, G.-J. Ahn, H. Hu, S.S. Yau, H.G. An, S. Chen, Dynamic audit services for outsourced storage in clouds, *IEEE Transact. Serv. Comput.*, accepted.
- [12] N. Cao, S. Yu, Z. Yang, W. Lou, Band Y. T. Hou, LT codes based secure and reliable cloud storage service, In: *Proceedings of IEEE INFOCOM 2012* (2012), 693–701.

