ISSN(Online): 2320 - 9801
ISSN (Print) : 2320 - 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

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

R.Krishnaveni[1], Dr.S.Dhanalakshmi[2]

Research Scholar, Department of Computer Science, Vivekanandha College of Arts and Sciences for Women (Autonomous), Elayampalayam, Tiruchengode, Namakkal, India

Head & Professor, Department of Computer Science, Vivekanandha College of Arts and Sciences for Women (Autonomous), Elayampalayam, Tiruchengode, Namakkal,India

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.

KEYWORDS: Public auditing, shared data, user revocation, cloud computing.

I. INTRODUCTION

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. 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 [2], [3].To protect the integrity of data in the cloud, a number of mechanisms [3]–[15] 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[3]).

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 [3]–[13] focus on auditing the integrity of personal data. Different from these works, several recent works [14], [15] 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. Due to the modifications from different users, different blocks are signed by different users. For security reasons, when a user leaves the group or misbehaves, this

DOI: 10.15680/IJIRCCE.2016. 0406024

user must be revoked from the group. As a result, this revoked user should no longer be able to access and modify shared data, and the signatures generated by this revoked user are no longer valid to the group[16]. Therefore, although the content of shared data is not changed during user revocation, the blocks, which were previously signed by the revoked user, still need to be re-signed by an existing user in the group. As a result, the integrity of the entire data can still be verified with the public keys of existing users only.

Since shared data is outsourced to the cloud and users no longer store it on local devices, a straightforward method to re-compute these signatures during user revocation (as shown in Fig. 1) is to ask an existing user (i.e., Alice) to first download the blocks previously signed by the revoked user (i.e., Bob), verify the correctness of these blocks, then re-sign these blocks, and finally upload the new signatures to the cloud. However, this straightforward method may cost the existing user a huge amount of communication and computation resources by downloading and verifying blocks, and by re-computing and uploading signatures, especially whenthe number of re-signed blocks is quite large or the membership of the group is frequently changing. To make this matter even worse, existing users may access their data sharing services provided by the cloud with resource limited devices, such as mobile phones, which further prevents existing users from maintaining the correctness of shared data efficiently during user revocation.

II. EXISTING SYSTEM

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.

Disadvantages Of Existing System:

- Especially when the number of re-signed blocks is quite large.
- Existing users may access their data sharing services provided by the cloud with resource limited devices, such as mobile phones.
- Frequent Security Issues.

III. PROPOSED SYSTEM

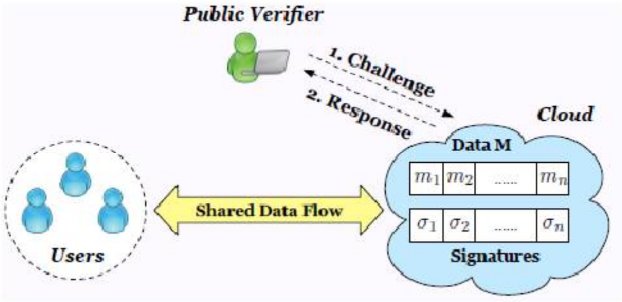
We propose Panda, a novel public auditing mechanism for the integrity of shared data with efficient user revocation in the cloud. In our mechanism, by utilizing the idea of proxy re-signatures, once a user in the group is revoked, the cloud is able to resign the blocks, which were signed by the revoked user, with a re-signing key. As a result, the efficiency of user revocation can be significantly improved, and computation and communication resources of existing users can be easily saved. Meanwhile, the cloud, which is not in the same trusted domain with each user, is only able to convert a signature of the revoked user into a signature of an existing user on the same block, but it cannot sign arbitrary blocks on behalf of either the revoked user or an existing user. By designing a new proxy re-signature scheme with nice properties, which traditional proxy re signatures do no have, our mechanism is always able to check the integrity of shared data without retrieving the entire data from the cloud.

Advantages:

- Easily Revocable of signatures for the existing users.
- The public verifier can audit the integrity of shared data without retrieving the entire data from the cloud.

DOI: 10.15680/IJIRCCE.2016. 0406024

IV. SYSTEM ARCHITECTURE



V. OVERVIEW

This project assume the cloud itself is semi-trusted, which means it follows protocols and does not pollute data integrity actively as a malicious adversary, but it 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. To protect the integrity of shared data, each block in shared data is attached with a signature, which is computed by one of the users in the group. Specifically, when shared data is initially created by the original user in the cloud, all the signatures on shared data are computed by the original user. After that, once a user modifies a block, this user also needs to sign the modified block with his/her own private key. By sharing data among a group of users, different blocks may be signed by different users due to modifications from different users. When a user in the group leaves or misbehaves, the group needs to revoke this user. Generally, as the creator of shared data, the original user acts as the group manager and is able to revoke users on behalf of the group. Once a user is revoked, the signatures computed by this revoked user become invalid to the group, and the blocks that were previously signed by this revoked user should be re-signed by an existing user's private key, so that the correctness of the entire data can still be verified with the public keys of existing users only.

Design Objectives:

Our proposed mechanism should achieve the following properties:

A) **Correctness***:* The public verifier is able to correctly check the integrity of shared data.

B) Efficient and Secure User Revocation:

On one hand, once a user is revoked from the group, the blocks signed by the revoked user can be efficiently re-signed. On the other hand, only existing users in the group can generate valid signatures on shared data, and the revoked user can no longer compute valid signatures on shared data.

C) Public Auditing:

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.

D) Scalability:

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

VI. MODULE DESCRIPTION

User Module:

- Registration
- File Upload
- Download
- Re-upload
- Unblock module

***Auditor Module**:*

- File Verification module
- View File

***Admin Module**:*

- View Files
- Block user

A) User Module

Registration:

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

***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.

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 reupload the block of file into cloud server with encryption .This ensure the files to be protected from unauthorized user.

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.

Unblock Module:

This module allows 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.

B) Auditor Module

***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.

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

C) Admin Module

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

Block User: In this module admin block the misbehave user account to protect the integrity of shared data

VII. SYSTEM IMPLEMENTATION

Basically, in the multi-parent idea when a message arrives to a node in the network, depending on its arrival time it chooses the fastest path in the network to get to its destination. When two parents (mother and father) are assigned to each node, if the mother is awake, the father can sleep and vice versa and the child node does not see any difference from a single-parent case. The base station belongs to all groups so it should wake up in all frames.

DOI: 10.15680/IJIRCCE.2016. 0406024

Procedural is a handler for the event of detecting a target, which can be triggered by an interrupt that is raised on sensing something.

VIII. CONCLUSION

This 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] B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revoation in the Cloud," in the Proceedings of IEEE INFOCOM 2013, 2013, pp. 2904–2912.
[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz,A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Communications of theACM, vol. 53, no. 4, pp. 50–58, Apirl 2010.
[3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson,and D. Song, "Provable Data Possession at Untrusted Stores," in the Proceedings of ACM CCS 2007, 2007, pp. 598–610.
[4] H. Shacham and B. Waters, "Compact Proofs of Retrievability,"in the Proceedings of ASIACRYPT 2008. Springer-Verlag,2008,pp. 90–107.
[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data StorageSecurity in Cloud Computing," in the Proceedings of ACM/IEEE IWQoS 2009, 2009, pp. 1–9.
[6] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling PublicVerifiability and Data Dynamic for Storage Security in Cloud Computing," in the Proceedings of ESORICS 2009. Springer-Verlag,2009, pp. 355–370.
[7] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-PreservingPublic Auditing for Data Storage Security in Cloud Computing," in the Proceedings of IEEE INFOCOM 2010, 2010, pp. 525–533.
[8] Y. Zhu, H.Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "DynamicAudit Services for Integrity Verification of Outsourced Storage in Clouds," in the Proceedings of ACM SAC 2011, 2011, pp. 1550–1557.
[9] C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220–232, 2011.
[10] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and S. Chen,"Dynamic Audit Services for Outsourced Storage in Clouds," IEEE Transactions on Services Computing, accepted.
[11] N. Cao, S. Yu, Z. Yang, W. Lou, and Y. T. Hou, "LT Codes-basedSecure and Reliable Cloud Storage Service," in the Proceedings of IEEE INFOCOM 2012, 2012, pp. 693–701.
[12] J. Yuan and S. Yu, "Proofs of Retrievability with Public Verifiability and Constant Communication Cost in Cloud," in Proceedings of ACM ASIACCS-SCC'13, 2013.
[13] H. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Transactions on Services Computing, accepted.
[14] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," in the Proceedings of IEEE Cloud 2012, 2012, pp. 295–302.
[15] S. R. Tate, R. Vishwanathan, and L. Everhart, "Multi-user Dynamic Proofs of Data Possession Using Trusted Hardware," in Proceedings of ACM CODASPY'13, 2013, pp. 353–364.
[16] B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud," in the Proceedings of ACNS 2012, June 2012, pp. 507–525.

BIOGRAPHY

R.Krishnaveni.,M.Sc., M.Phil., Research Scholar, Department of Computer Science, Vivekanandha College of Arts and Sciences for Women (Autonomous),Elayampalayam, Tiruchengode, Namakkal -dt.

Dr.S.Dhanalakshmi. s,MCA.,M.Phil.,Ph.D,ME, Prof&Head of Department of computer science and computer application, Vivekanandha College of Arts and Sciences for Women (Autonomous), Elayampalayam,Tiruchengode, Namakkal-dt.