International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 09 | Dec-2015 www.irjet.net p-ISSN: 2395-0072

PUBLIC AUDITING FOR SHARED DATA WITH EFFICIENT MANNER IN CLOUD

Ms.Zaibunnisa S, Mrs.Sasidevi J, Mrs.Shobana M, Mrs.Divyamala A

Student, Dept. of Comp.Sci, Dhanalakshmi Srinivasan Engineering College, Tamilnadu, India
Assistant Professor,Dept. of Comp.Sci, Dhanalakshmi Srinivasan Engineering College,Tamilnadu,India
Assistant Professor,Dept of Comp.Sci, Dhanalakshmi Srinivasan Engineering College,Tamilnadu,India
Student, Dept. of Comp.Sci, Dhanalakshmi Srinivasan Engineering College, Tamilnadu, India

----------*****----------

Abstract - ***Cloud computing is defined as a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. In existing once a user is revoked from the group, the blocks which were previously signed by this revoked user must be re-signed by a cloud using proxy resignatures but the content of the block remains same. This straightforward method, which allows a cloud to resign blocks on behalf of existing users during user revocation. To check data integrity public verifier has to download entire data from the block and verify it. This is inefficient due to the large size of shared data in the cloud. In proposed, the sharing of data between users in a group with highly secure manner in the cloud. An authorized member in a group must access the shared data using AES algorithm and Random key generation process. During user revocation the block is not resigned by a cloud but the block is allocated to a revoked user within a time period otherwise the block is completely deleted. Also the public verifier is able to verify the integrity of shared data without retrieving the entire data from the cloud. Identity of the signer on each block in shared data is kept private from the public verifier. This mechanism also includes a novel public auditing mechanism for the integrity of shared data with efficient user revocation in mind. This mechanism is in a position to perform multiple auditing tasks at the same time rather than corroboratory them one by one.***

Key words: *Cloud Computing,User Revocation, Resignatures,*

1.INTRODUCTION

With data storage and sharing services (such as Dropbox 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 .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, that user 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 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.

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 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 when the 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.

2.SYSTEM MODEL

In this section we consider the existing system design and the proposed system.

2.1 Existing System

In existing once a user is revoked from the group, the block which were previously signed by this revoked user must be re-signed by a cloud using proxy resignatures, but the content of the block remains same. This is inefficient due to the large size of shared data in the cloud. This method is insecure because the private data of revoked user is misused by an existing user. The sharing of data between users in a group is not highly secure. To check data integrity public verifier has to download entire data from the cloud and verify it.

Problem Identified

- Need to verify large number of blocks and re-signed signatures.
- Cost is high for implement the straightforward method.
- The revoked user can access the data with help of existing sign in the group.

2.2 Proposed System

In this proposed system the sharing of data between users in a group with highly secure manner in the cloud. An authorized member in a group must access the shared data using AES algorithm and Random key generation process. During user revocation the block is not resigned by a cloud but the block is allocated to a revoked user within a time period otherwise the block is completely deleted.

Also the public verifier is able to verify the integrity of shared data without retrieving the entire data from the cloud. Identity of the signer on each block in shared data is kept private from the public verifier.This method also supports a novel public auditing mechanism for the integrity of shared data with efficient user revocation in cloud.

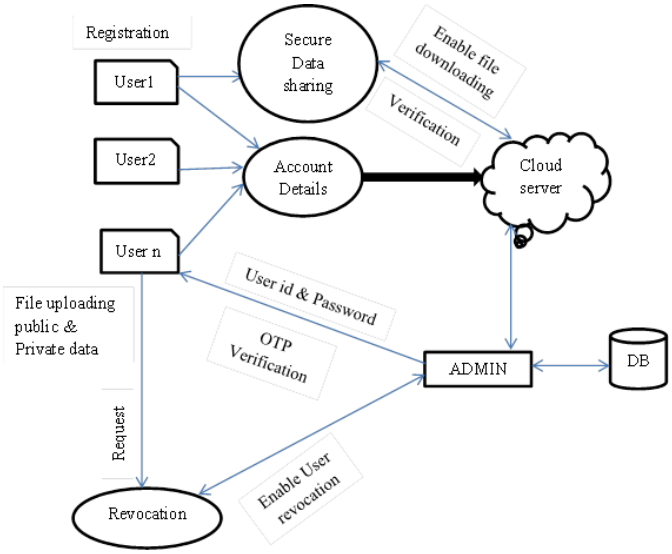

Fig-1: System Design

Benefits

- Cloud data can be efficiently shared among a large number of cloud users.
- It does not pollute data integrity.
- The revoked user is not able to collude with the cloud easily.
- Login with secret key in each time.

3.DESIGN CONSTRUCTION

This Section consists of the following module design to form an efficient user revocation and public auditing. These are to be explained in this section.

3.1 User Registration

In this module, the user registration process is done by the admin. Here every user's give their personal details for registration process. After registration every user will get an ID for accessing the cloud space. If any of the user wants to edit their information they have submit

the details to the admin after that the admin will do the edit and update information process. This process is controlled by the Admin.

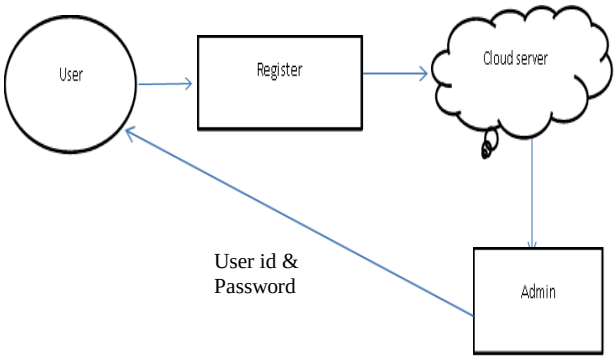

Fig-2: User Registration

3.2 File Uploading

An information shared by the user in the cloud is encrypted by using AES (Advanced Encryption Standard) algorithm. All of the information shared by every user is encrypted and stored in the cloud. The encrypted data is decrypted by the user, using the public key of owner of the data. Decryption is the process of converting cipher text into plain text. AES algorithm is used for encrypting and decrypting the information. The user can view the data and also can download the data with admin verification which provides high security in cloud.

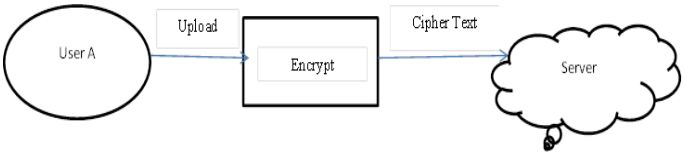

Fig-3: Encryption

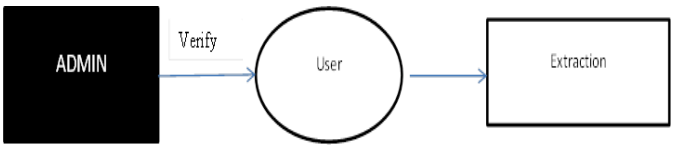

Fig-4: Decryption

3.3 Data Forwarding

The encrypted data or information stored in the cloud is forwarded to another user account by using that user's secret key. If any user wants to access public data they can directly access from the cloud. The private data can be forwarded to another user with random secret key. Before downloading the data the receiver must be verified by admin. This method create download access to authenticated user.

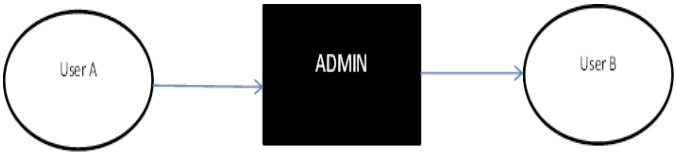

Fig-5: Data Forwarding

3.4 User Revocation

In this module, if any user wants to revoked from the cloud, that user request for revocation is sends to admin. After admin verification that user must be revoked from the cloud. During revocation user details can be deleted from the database but Uploaded files of revoked user is maintained during user revocation.

4 CONCLUSION

This proposed method has concluded secure data sharing with efficient user revocation in the cloud. Only authorized member must access the shared data from the cloud. Without downloading entire data from the cloud, the public verifier is able to check the integrity shared data from the cloud. By only admin verification user must be revoked from the cloud.

4.1 FUTURE ENHANCEMENT

Designing an efficient public auditing mechanism with the capabilities of reserving identity privacy and supporting traceability is still open. Another problem is data freshness. Traceability which means the ability for the group manager (i.e., the original user) to reveal the identity of the signer based on verification metadata in some special situations. The user must be given complete access control over the published data. Also, powerful security mechanisms must always supplement every cloud application. Attaining all these would end up in achieving the long dreamt vision of secured Cloud Computing in the nearest future.

REFERENCES

[1] Armbrust M., Fox A., Griffith R., 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," Comm. ACM, vol. 53, no. 4, pp. 50-58.

[2] Ateniese G., Burns R., Curtmola R., Herring J., Kissner L., Peterson Z.and Song D.(2007), "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS'07), pp. 598-610.

[3] Ferrara A.L., Green M., Hohenberger S. and Pedersen M.O.(2009),"Practical Short Signature Batch Verification," Proc. Cryptographers'Track

at the RSA Conf. Topics in Cryptology CT-RSA'09), pp. 309-324.

[4] Shacham H. and Waters B.(2008), "Compact Proofs of Retrievability," Proc. 14th Int'l Conf. "Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT'08)", pp. 90- 107.

[5] van Dijk M., Juels A., Oprea A., Rivest R.L.,Stefanov E. and Triandopoulos N.(2012), "Hourglass Schemes: How to Prove That Cloud Files are Encrypted," Proc. ACM Conf. Computer and Comm. Security (CCS'12), pp. 265-280.

[6] Wang B., Li B. and Li H.(2013), "Public Auditing for Shared Data with Efficient User Revocation in the Cloud," Proc. IEEE INFOCOM, pp. 2904-2912.

[7] Wang C., Wang Q., Ren K. and Lou W.(2009), "Ensuring Data Storage Security in Cloud Computing," Proc. 17th ACM/IEEE Int'l Workshop Quality of Service (IWQoS'09), pp. 1-9.

[8] Xu L., Wu X. and Zhang X.(2012), "CL-PRE: A Certificateless Proxy Re-Encryption Scheme for Secure Data Sharing with Public Cloud,"Proc. Seventh ACM Symp. Information, Computer and Comm. Security(ASIACCS'12), pp. 87-88.

[9] Yuan J. and Yu S.(2014)," Efficient Public Integrity Checking for Cloud Data Sharing with Multi-User Modification",http://eprint.iacr.org/2013/484.