ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 4, Issue 3 (Jul. - Sept. 2016)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2016)

Design of Management of User Revocation with Public Auditing for Shared Data in the Cloud

Anju T G
PG Scholar, Dept. of CSE, Vidya Academy of Science and Technology, Thrissur, India

Abstract
Cloud computing is one of the biggest innovation which uses advanced computational power and it improves data sharing and data storing capabilities. Main difficulty with cloud computing was data integrity, data privacy and data access by unauthorised users. With data storage and sharing services provided by the cloud,users can easily modify and share data as agroup. To verify integrity of the shared data, members in the group needs tocompute signatures on all shared data blocks. Different blocks in shared data are generally signed by different users due to data modifications performed bydifferent users . User revocation is one of the biggest security issue in groups.During user revocation shared data block signed by revoked user needs to download and resign by existing user. This task is very difficult due to the large size of shared data blocks on cloud. Proxy resignatures concept whichallows the cloud to resign blocks on behalf of existing users during user revocation, so that downloading of shared data blocks is not required. In addition a public auditor who can audits the integrity of shared data without retrieving the entire data from the cloud.

Keywords
Cloud computing, User revocation,Data integrity,Public auditing.

I. Introduction

With the data storage and sharing services provided by the cloud people can worktogether as a group. Once a user creates shared data in the cloud, each user in the group can access and modify the shared data as they wish.

Although cloud providers promise a more secure and reliable environment to the users, the integrity of data in the cloud may still be compromised. To preserve the data integrity in the cloud a signature is attached to each block in data and the integrity of data relies on the correctness of all the signatures. With the shared data in the group once a user modifies a block ,the user needs to compute a signature for the modified block. The signature computed by using the users private key which is generated during the user registration.Due to the modifications from different users, different blocks are signed by different users. when a user leaves the group, 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 resigned by an existing user in the group.Proxy resignature scheme is used for the same. As a result, the integrity of the entire data can still be verified with the public keys of existing users only. And the efficiency of user revo cation can be significantly improved, and computation and communication resources of existing users can be easily saved. 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 resigned by the cloud.

Overview

To preserve the integrity of shared data with efficient user revocation in the cloud a novel public auditing mechanism used by utilizing the idea of proxy resignatures . 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 resigning key .To protect the integrity of data in the cloud and performs the auditing mechanism, a number of techniques have been proposed. Like MAC, HLA etc.

MAC Based Solution : MAC based technique is used for the data authentication. In this user upload data blocks with MAC and the Cloud provider provides Secret key to TPA. Here TPA will retrieve data blocks randomly and MAC uses SK to check the correctness of data. Online burden to users due to limited use (i.e. Bounded usage) and stateful verification is the main limitation of this method.

Using EAP : Using EAP they proposed identity based signature for hierarchical architecture. They provide an authentication protocol for cloud computing (APCC) . As compare to SSL authentication protocol APCC is more lightweight and efficient. It also used Challenge handshake authentication protocol (CHAP) for authentication. By using EAP, first the client request for any service to cloud service provider , then SPA send a CHAP request or a challenge to the client. When client recieves the challenge, client will sends CHAP response which is calculated by using the hash function to SPA. And finally SPA checks the challenge value with its own calculated value . If they are matched then SPA sends CHAP success message to the client.

Using Automatic Protocol Blocker : Automatic Protocol Blocker technique for error correction which checks data storage correctness . When an unauthorized user access user data, a small application runs which monitors user inputs, It matches the user input, if it is matched then it allow user to access the data otherwise it will block protocol automatically. Automatic protocol technique have five algorithms as keygen , SinGen, GenProof, VerifyProof ,Protocol Verifier. Protocol Verifier is used by CS. It contains three phases as Setup, Audit and Pblock.

Using Virtual Machine : when user request CSP for service CSP authenticate the client and provide a virtual machine by means of Software as a service. Virtual Machine (VM) uses RSA algorithm for cryptography, where client encrypt and decrypt the file. SHA-512 algorithm is also used for making the message digest and check the integrity of data. This also helps in avoiding unauthorised access and providing privacy and consistency. Limitation to this technique is it is useful only for SaaS model.

Unless by using the above techinques a Homomorphic

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

authenticators also called homomorphic verifiable tags, allow a public verifier to check the integrity of data stored in the cloud without downloading the entire data. Besides unforgeability (only a user with a private key can generate valid signatures), a homomorphic authenticable signature scheme, which denotes a homomorphic authenticator scheme based on signatures.

Design

Management of User Revocation With Public Auditing For Shared Data in the Cloud includes mainly 3 entities 5 algorithms.
The 3 entities are::

- Cloud
- Public verifier
- Users(whoshare data as a groups)

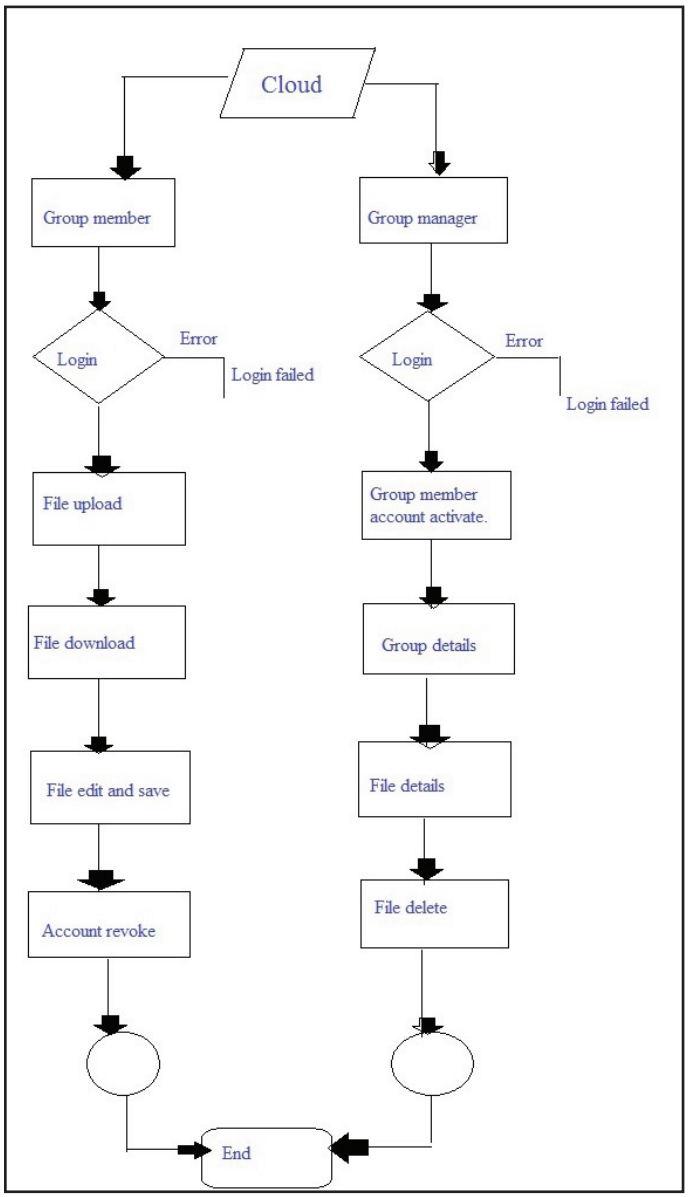
Algorithms are::

- KeyGen(Key generation)
- ReKey(Re-sign key generation)
- Sign(signing)
- Sign (Resigning)
- Verify(Verification)

Key Generation::
During the new user registration process the original user(Group manager) generates a public and private key pair for the new user. Without the loss of generality the original user generates a user list which contains the id's of all the users in the group.The user list is public.
Resign key generation::
In the re-sign key generation the cloud computes a re-signing key for each pair of users in the group.Frst proxy generates a random number " r " and send it to user u1. User u1 computes r/a and send it to the user u2. And user u2 calculates rb/a and send to the proxy and the proxy recovers b/a.
Signing::
When the original user creates shared data in the cloud, he/she computes a signature on each block as in Sign. THe signature on each block is calculated by using the private key of the user and the block identifier . If a user in the group modifies a block in shared data, the signature on the modified block is also computed as in Sign.
Re-signing::
In ReSign, a user is revoked from the group, and the cloud re-signs the blocks, which were previously signed by this revoked user,with a re-signing key. For the re-signing process cloud uses public key ,signature on the block and block identifier. And proxy checks hash function of these three is equals whether 1 or not. If it outputs "1" Re-signing performes.after that the name of the revoked user is removed from the user list.
In ReSign, without loss of generality, we assume that the cloud always converts signatures of a revoked user into sig- natures of the original user. The reason is that the original user acts as the group manager, and we assume he/she is secure in our mechanism. Another way to decide which re-signing key should be used when a user is revoked from the group, is to ask the original user to create a priority list (PL). Every existing user's id is in the PL and listed in the order of re-signing priority. When the cloud needs to decide which existing user the signatures should be converted into, the first user shown in the PL is selected. To ensure the cor- rectness of the PL, it should be signed with the private key of the original user (i.e., the group manager).

Verification::
The verification on data integrity is performed via a challenge-and-response protocol between the cloud and a public verifier. More specifically, the cloud is able to generate a proof of possession of shared data in ProofGen under the challenge of a public verifier. In Proof- Verify, a public verifier is able to check the correctness of a proof responded by the cloud.
By using the auditing messag , auditing proof and existing users public key public verifier checks the correctness of the shared data. If the result is 1 the verifier believes the integrity of the blocks on shared data is correct.

Block Diagram of Design::



The above architecture of design shows that under the cloud module ,there are two modules.

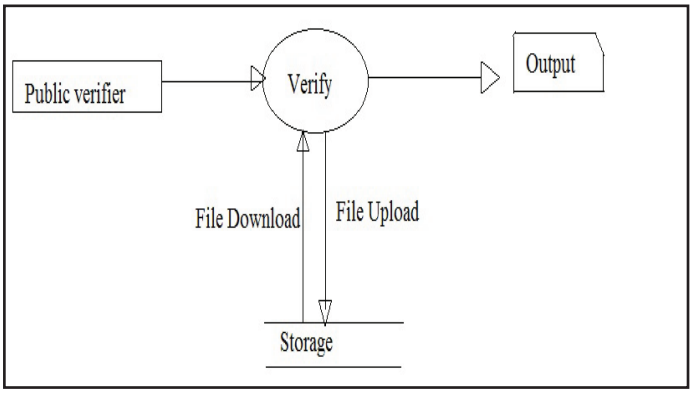
1.Group Manager module
2.Group member module

Both can login using their login details. After successful login, Group Manager activates newly added members of the cloud. He can also check the group details , file details of the cloud and he can also delete the files . After successful login, Group

Member's signature is verified. After successful verification, the member can upload, download and can modify the files. The Group Member's account can be revoked after he leaves the cloud by the Group Manager. If the login fails, due to the wrong login details, both in Group Member and Group Manager modules, an error is generated. Because of which neither Manager nor Member can login. During group signature verification in the Group Member module, if the verified result turns out to be false, it is treated as an error and the Member has no access over the group. . 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.

The last module is the auditor module. Auditor(Public verifier) Module is responsible for following operation.

- Verification of Files: The public verifier is responsible for checking the scalability of shared data.
- Files View: This module allow auditor to view the all details of file upload, file download, blocked user, re-upload.



Conclusion

The public auditing for share ddata with efficient user revocation in the cloud ,proposed a new public auditing mechanism for shared datawith efffcient user revocation in the cloud. When a user in the group is revoked, It allow the semi-trusted cloud to re-sign blocks that were signed by the revoked user with proxy re-signatures. The cloud can improve the efciency of user revocation by using the Proxy resignature scheme,and existing users in the group can save a signicant amount of computation and communication resources during user revocation.

References

[1] *M. Blaze, G. Bleumer, and M. Strauss, Divertible Protocols and Atomic Proxy Cryptography, Proc. Intl Conf. the Theory and Application of Cryp- tographic Techniques (EUROCRYPT98), pp. 127- 144, 1998*

[2] *M. Armbrust, A. Fox, R. Grifth, A.D. Joseph, R.H. Katz, A. Kon- winski, G. Lee,D.A.Patterson,A.Rabkin,I.Stoica,andM. Zaha-ria,AViewofCloud Computing, Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.*

[3] *G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peter- son, and D. Song, Provable Data Possession at Untrusted Stores, Proc. 14th ACM Conf. Computer and Comm. Security (CCS07), pp. 598-610, 2007*

[4] *H. Shacham and B. Waters, Compact Proofs of Retrievability, Proc. 14th Intl Conf.TheoryandApplicationofCryptolo gyandInfor-mationSecurity: Ad- vances in Cryptology (ASIACRYPT08), pp. 90- 107, 2008*

[5] *C. Wang, Q. Wang, K. Ren, and W. Lou, Ensuring Data Storage Security in CloudComputing,Proc.17thACM/ IEEEIntlWork-shopQualityofService (IWQoS09), pp. 1-9, 2009*

[6] *Q.Wang,C.Wang,J.Li,K.Ren,andW.Lou,EnablingPublicVeri abilityand DataDynamicforStorageSecurityinCloudComputing,Proc.14thEuropean Conf. Research in Computer Security (ESORICS09), pp. 355-370, 2009*

[7] *C.Wang,Q.Wang,K.Ren,andW.Lou,Privacy-PreservingPublicAuditing for Data Storage Security in Cloud Computing, Proc. IEEE INFOCOM, pp. 525-533, 2010.*

[8] *Y.Zhu,H.Wang,Z.Hu,G.-J.Ahn,H.Hu,and S.S.Yau, Dynamic AuditSer- vices for Integrity Verication of Outsourced Storages in Clouds, Proc. ACM Symp. Applied Computing (SAC11), pp. 1550-1557, 2011*

[9] *C. Wang, Q. Wang, K. Ren, and W. Lou, Towards Secure and Dependable StorageServicesinCloudComputing,IEEETrans.ServicesComputing,vol. 5, no. 2, pp. 220-232, Jan. 2012.*

[10] *Y. Zhu, G.-J. Ahn, H. Hu, S.S. Yau, H.G. An, and C.-J. Hu, Dynamic Audit Services for Outsourced Storages in Clouds, IEEE Trans. Services Comput- ing, vol. 6, no. 2, pp. 227-238, Apr.- June 2013*

[11] *N. Cao, S. Yu, Z. Yang, W. Lou, and Y.T. Hou, LT Codes-Based Secure and ReliableCloudStorageService,Proc.IEEEINFOCOM,pp.693-701,2012.*

[12] *J. Yuan and S. Yu, Proofs of Retrievability with Public Veriabil- ity and Con- stant Communication Cost in Cloud, Proc. ACM Intl Workshop Security in Cloud Computing (ASIACCS-SCC13), pp. 19- 26, 2013*

[13] *H. Wang, Proxy Provable Data Possession in Public Clouds, IEEE Trans. Services Computing, vol. 6, no. 4, pp. 551-559, Oct.- Dec. 2013*

[14] *B. Wang, B. Li, and H. Li, Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud, Proc. IEEE CLOUD, pp. 295-302, 2012.*

[15] *S.R. Tate, R. Vishwanathan, and L. Everhart, Multi-User Dynamic Proofs of Data Possession Using Trusted Hardware, Proc. Third ACM Conf. Data and Application Security and Privacy (CODASPY13), pp. 353-364, 2013*

[16] *B. Wang, B. Li, and H. Li, Knox: Privacy-Preserving Auditing for Shared DatawithLarge Groupsinthe Cloud,Proc.10thIntlConf. Applied Cryptog- raphy and Network Security (ACNS12), pp. 507-525, June 2012*