Files and Accounts Security for Multi-Owners in Cloud

Umme Sadiya
M.Tech (Computer Science & Engg)
HKBK College of Engineering
Bangalore, India
sadiyakhan55@gmail.com

Abstract— **Advances in networking technology and an increase in the need for computing resources have prompted many organizations to outsource their storage and computing needs. This new economic and computing model is commonly referred to as Cloud computing. Cloud computing enables its users to share the Group resources efficiently. Due to the frequent change of membership, preserving the data and identity is still a challenging issue. This paper proposes a secure multi-owner data sharing scheme, for dynamic Groups in the Cloud. For the Cloud users to share the data anonymously, we use the Group signature and Dynamic broadcast encryption technique.**

Keywords—Cloud computing, dynamic Groups, data sharing and privacy preserving.

I. Introduction

In Cloud computing [1], Cloud service providers such as Amazon, provides various services to the users. These users can migrate their local data into the Cloud and can enjoy high quality services of the Cloud. The most fundamental services offered by the Cloud service provider is data storage.

Considering an example, a company allows its users to share and store their files in the Cloud, either from the same or different Groups. By this Users can save significant investment on their local data management and can be released from the troubles caused by it. But how can they trust the Cloud servers that are managed by the Cloud providers? The data that is stored by the Users can be sensitive, such as business plans or other confidential data. These data can be stolen, modified or misused by other rival companies. The basic solution to preserve the privacy would be encryption. The encrypted files can be uploaded into the Cloud. It is an easy task to design an efficient secure system due to some following issues-

First identity privacy. Without ensuring their privacy Users may be unwilling to store or share the data into the Cloud. Second, in a multi-owner fashion, any member should be able to enjoy the data storing and sharing services provided by the Cloud. It is more flexible compared to single-owner access in practical applications. Lastly, when a new staff participates or current employee cancellation and replacement, they can learn the content of the data uploaded before their participation such that they could not have to contact data owners to obtain all the decryption keys.

To overcome these issues we try to propose secure multi-owner data sharing scheme which is also able to provide:

1. Secure multi-owner data sharing scheme, where any User of the Group can be able to enjoy the services provided by the Cloud.
2. Secure and privacy preserving access to Users, where any user can share the file hiding their identities from untrusted Cloud.
3. Support to the dynamic Groups efficiently, where a new User can access the file uploaded before their participation.

This paper is organized as follows:

Section 2 overviews the related work. In section 3, algorithms and its steps are reviewed. In section 4, finally we conclude the paper.

II. Related Work

In [6], specifically the blocks of contents were encrypted using symmetric content keys by the data owner. The master public key was used to encrypt again these content keys. For access control, the server uses proxy cryptography to directly re-encrypt the content keys. But the problem was collusion attack between the malicious user and the untrusted server can be happen through which it is possible to learn the decryption keys of all the encrypted blocks.

In [7], the paper is based upon Group signature and cipher text policy attribute-based encryption technique. Each user will obtain two keys after registration: a Group signature key and an attribute key. Therefore the user can encrypt a data file using attribute-based encryption and the other Users in the Group can use attribute keys to decrypt the data. But the user revocation is not supported in this scheme.

In [4], the files were divided into file Groups and they were encrypted using a unique file-block key. Further this file-block key is encrypted using a lock-box key when data owner needs to share the file with the other Users. But the problem is, for large-scale data sharing there will be heavy key distribution overhead.

In [5], there were two parts in the file stored on the untrusted server (file metadata and the file data). The file metadata consists of the access control information. But here the user revocation is intractable for large-scale data sharing, because the file metadata needs to be updated frequently.

In[15], this paper enable to hide the identities of data owner's within an organization (Group) from any verifiers in the multi-owner scenario, where a data file is owned and can be modified by a number of Users. However, both of these two schemes introduce significant overheads on verification metadata to ensure anonymity.

In [3], Key Policy Attribute Based Encryption (KP-ABE) technique was used. The file was encrypted using the random key by the data owner; further random keys are encrypted using the set of attributes using KP-ABE. When the Group manager assigns an access structure and the corresponding secret key to the user, user can only decrypt the cipher text if and only if the data file attributes satisfy the access structure. However a single owner manner may hinder the application, where as any Group member should be able to store and share the data files with others.

In [18], a new concept called provable data possession (PDP) using hash index hierarchy and homomorphic verifiable response was defined. This method either unnecessarily reveals the identity of a data owner to the untrusted Cloud or any public verifiers or introduces significant overheads on verification metadata to preserve anonymity.

From the above analysis, we can observe that it is a challenging issue to securely share the data in a multi-owner manner while preserving identity from an untrusted Cloud. To overcome some of the above discussed problems, we try to propose a secure multi-owner data sharing scheme.

III. DESIGN AND SYSTEM MODEL

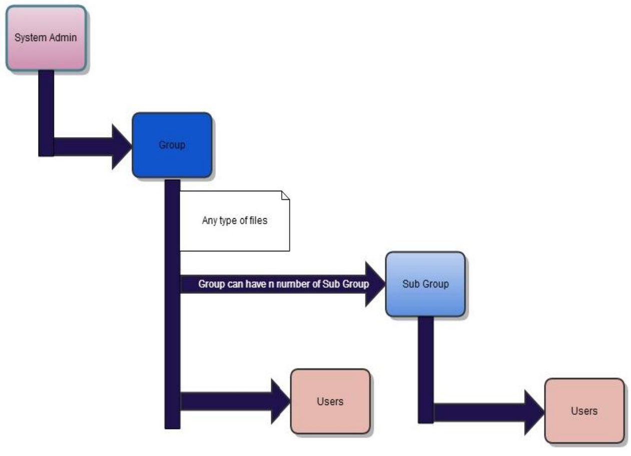


Fig. 1: System Model

We consider the Cloud computing by taking an example of the company that uses a Cloud to enable its users from same or different Group to share the files. The system model (Fig 1) consists of Cloud, System Admin, Group Admin, Users, Sub-groups as illustrated in Fig 1.

A. MODULES

The system consists of following modules-

1. User and Group management
2. Responsibilities of Group and System Admin
3. Key Generation
4. File Management
5. User permission management

1. User and Group Management: System Admin will be responsible for the creation of Group and Users. Group Admin is responsible for the creation of Sub-Groups. Users are created by System Admin only, but access permission to file is given by Group Admin.

2. Responsibilities of Group and System Admin: System Admin can only create Users and Groups. Access permission between Groups, Sub-Groups and Users can be done by Group Admin only. System Admin and Group Admin can upload any files. File uploaded by System Admin is visible to all Groups and Sub-Groups. But file uploaded by Group Admin is only visible to its particular Group and Sub-Group. Group Admin can give permission to the user who needs access to the file.

3. Key Generation: While creating a Group, User needs to enter his email ID and same needs to be verified. After verification of email ID only access key will be generated which will be sent to Group Admin email address. Group Admin needs to enter his secret key, which can be used in case if Group Admin forgets his access key. RSA algorithm is used to generate access key. Again when user needs to access the file uploaded by the Group Admin, he will get common key (common to all the users who access the file). Diffie–Hellman algorithm [20] is used to generate common key. MD5 or SHA is used for cryptography, to generate hash value.

4. File Management: Any uploaded file will have Read, Write and Delete permission. Group Admin assigns each file to User/Sub-Group to whom he wants to give access to the file. When the file is uploaded by System Admin or Group Admin, file will come to the user's queue. A unique common key is sent to user's mail ID. When User clicks on the link, he needs to enter his secret key and need to enter common key to access file.

5. Permission management: Permission will be given to user by Group Admin. Once User is deleted from the

System by System Admin, all rights given to each Group for each file will be revoked automatically.

B. DESIGN

Generating hash value

1. Check the validity of data.

2. Get the instances for a given digest scheme MD5 or SHA.

3.Generate the digest. Pass in the text as bytes, length to the bytes (offset) to be hashed; for full string pass 0 to text.length ().

4. Get the String representation of hash bytes, create a big integer out of bytes then convert it into hex value (16 as input to String method)

5. Return the digest.

Key management
Using Diffie-Hellman Algorithm

1. Global public elements Select any prime number: ’q’ Calculate the primitive root of q: ‘a’such that a<q

2. Asymmetric key generation by User ‘A’ Select a random number as the private key $X_{A,}$ where $X_A < q$ Calculate the public key $Y_A=a^{XA}$ mod q

3. Key Generation by User ‘B’ Select a random number as the private key $X_{B,}$ where $X_B < q$
Calculate the public key $Y_B=a^{XB}$ mod q

4. Exchange the values of public key between A & B

5. Symmetric key (K) generation by User A, K= Y_B^{XA} mod q

6. Symmetric key (K) generation by User B, K= Y_A^{XB} mod q

Using RSA Algorithm

1.Choose two distinct prime numbers p & q

2. Find n such that n=p * q

3. Find the quotient n, phi (n)
Phi (n) = (p-1)(q-1)

4. Choose an e such that 1<e<phi (n), e is kept as the public key exponent

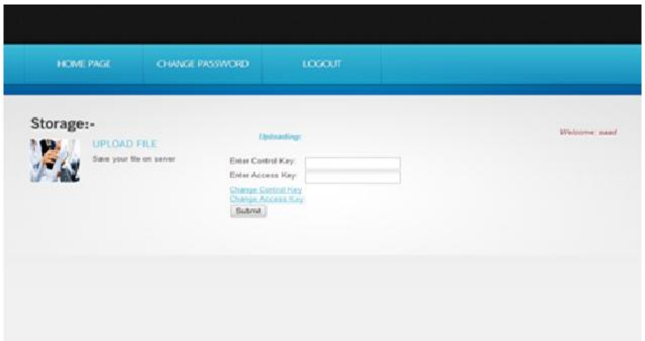
5.Determine d using modular arithmetic
d=1(mod phi(n))
d is kept as the private key exponent
6. For ciphertext C, C=m^e(modn)

7. For original message, m=C^d(modn)

IV. SIMULATION

This paper is simulated using java programming language. The simulation consists of 3 roles: System Admin, Group Admin, Users. The simulation is conducted in a laptop with Windows 2007 OS and Eclipse software. This paper consists of 5 modules. After simulation, it is deployed in a real Cloud Jelastic.

V. RESULT



Storage:-

Uploading:

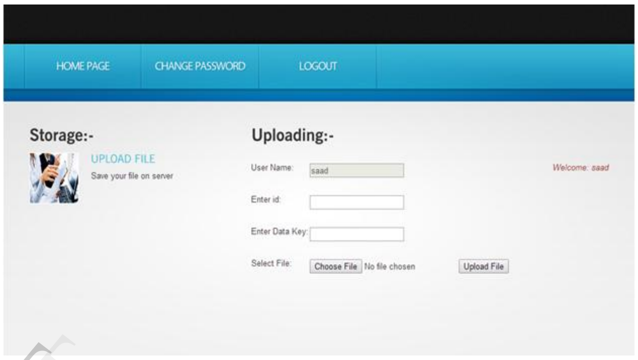
Welcome: saad

Enter Control Key:

Enter Access Key:

Change Control Key
Change Access Key

Submit



Storage:-

Uploading:-

User Name: saad

Welcome: saad

Enter id:

Enter Data Key:

Select File: Choose File No file chosen Upload File

REFERENCES

[1] 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,” Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[2] S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” Proc. Int’l Conf. Financial Cryptography and Data Security (FC), pp. 136- 149, Jan. 2010.

[3] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing,” Proc. IEEE INFOCOM, pp. 534-542, 2010.

[4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, “Plutus: Scalable Secure File Sharing on Untrusted Storage,” Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[5] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, “Sirius: Securing Remote Untrusted Storage,” Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.

[6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage,” Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.

[7] R. Lu, X. Lin, X. Liang, and X. Shen, “Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing,” Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[8] B. Waters, “Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,” Proc. Int’l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,” Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.

[10] D. Naor, M. Naor, and J.B. Lotspiech, “Revocation and Tracing Schemes for Stateless Receivers,” Proc. Ann. Int’l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.

[11] D. Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing,” Proc. Int’l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229, 2001.

[12] D. Boneh, X. Boyen, and H. Shacham, “Short Group Signature,” Proc. Int’l Cryptology Conf. Advances in Cryptology (CRYPTO),pp. 41-55, 2004.

[13] D. Boneh, X. Boyen, and E. Goh, “Hierarchical Identity Based Encryption with Constant Size Ciphertext,” Proc. Ann. Int’l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.

[14] BRODKIN, J., “Loss of customer data spur closure of online storage service.” The linkup”, Network world (Aug 2008).

[15] B.WANG,b.Li,”Knox:Privacy-preserving auding for shared data with large groups in the Cloud,” proc. 10th Int'l conf.Applied Cryptography and NETWORK security,pp.507-525,2012.

[16] R.Dingledine, N.Mathewson, P.Syrerson,”Tor: The second-Generation Onion Router,” Int'l conf, (Aug 2009).

[17] B. wang,Sherman M.M.Chow,Mingli and H. Li,”Storin Cloud via security-mediator in IEEE,2013,33rd Int’l Conf,Distributed computing system.

[18] C.Anand 1, Prabu.P 2, R.Prasath.V 3, Sasikumar.P 4, Silambarasan.P5, Mr.P.Sivakumar,” Verifying Integrity and Availability in Multi-Cloud Using PDP”, International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 2, Issue. 4, April 2013, pg.84 – 87 .

[19]C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy - Preserving Public Auditing for Data Storage Security in Cloud Computing,” Proc. IEEE INFOCOM, pp. 525-533, 2010.

[20]X Liu, Y. Zhang, B. Wang, and J.Yan, “Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud”, IEEE transactions on parallel and distributed systems, vol. 24, no. 6, june 2013.