International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 23 Issue 7 –OCTOBER 2016.

Data Sharing Schema for Dynamic Groups in Cloud Using Secure Anti-Collusion

ZEBA FATHIMA MOHAMMED[#1] and CH.LAVANYA SUSANNA[*2]

[#] *M.Tech (CSE), Nimra College of Engineering & Technology, A.P., India.*

[*] *Assistant Professor, Dept. of Computer Science & Engineering, Nimra College of Engineering & Technology, A.P., India.*

***Abstract*— Cloud computing now a day is increasing over the last few years due to its attractive features like scalability, flexibility, low cost and easy start up for the beginners. It provides effective security of the data and information in the cloud storage. The data Distribution in many users accessing for dynamic groups preserves data and its identity and privacy from an untrusted cloud and grants access to frequent change of membership. Users can attain an effective and economical approach of scheme for data sharing among group members in the cloud. It is an advantage of low maintenance and little management cost. Meanwhile, we provide security guarantees for the sharing data files since they are outsourced. A secure communication channel for existing schemes channel is a strong assumption and is difficult for practice. In this paper, we propose a secure data sharing scheme for dynamic members. First, we propose a secure way for key distribution without any secure communication channels. Second, our scheme can achieve fine-grained access control, any user in the group can use the source in the cloud and revoked users cannot access the cloud again. Third, we can protect the scheme from collusion attack, which means that revoked users cannot get the original data.**

Index Terms*— Cloud computing, anti-collusion, group manager, group user, Access control, privacy-preserving, key distribution

I. INTRODUCTION

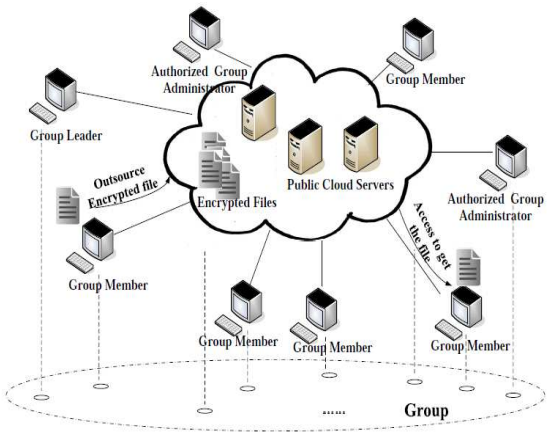
One of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application. A company allows its staffs in the same group or department to store and share files in the cloud. However, it also poses a significant risk to the confidentiality of those stored files. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. and efficient data sharing scheme, especially for dynamic groups in the cloud. Benefited from cloud computing, users can achieve an effective and economical approach for data sharing among group members in the cloud with the characters of low maintenance and little management cost. Unfortunately, because of the frequent change of the membership, sharing data while providing privacy-preserving is still a challenging issue, especially for an untrusted cloud due to the collusion attack. Meanwhile, we must provide security guarantees for the sharing data files since they are outsourced. The examples of cloud computing include available backup services, dynamic social networking services, and individual data services, etc. The Cloud computing also includes online applications, such as those accessible through Microsoft Online Services. The hardware services, similar as redundant servers, mirrored websites or files, and Internet based clusters are also examples of cloud computing. The services offered by the Cloud Computing are also called as on demand computing, utility computing's or pay as we need to go computing. The services offered by the cloud are Saas (Software as a service), Paas (Platform as Services), Iaas (Infrastructure as Services). The deployment models of cloud are Private Clouds, Public Clouds, Hybrid Clouds and Community Clouds. The cloud computing security is a definite set of control based technologies and policies designed to observe to monitoring the submission of rules and protect the information and its data, application and infrastructure linked with cloud computing to use. There are two issues in the security of the cloud are Security issue faced by Cloud Service Provider (CSP) and security issue faced by the users.

II. PROPOSED SYSTEM

Since the number of users revoked is independent of the operations of the members to decrypt the data files almost remain same. Again the cost is not dependent on the number of users revoked. Because, the file upload in this schema consists of two verifications for signature. The user can obtain the private key safely from group manager Certificate Authorities and secure communication channels. This scheme supports the dynamic group efficiently, as in the private key of any user need not to be changed when a user is revoked. The main contributions of our scheme include:

1) We provide a secure way for key distribution with-out any secure communication channels. The users can securely obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user. 2) Our scheme can achieve fine-grained access control, with the help of the group user list, any user in

the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked. Cloud is operated by Cloud Service Providers (CSPs) which provides abundant storage services. However, the cloud is not fully trusted Similar to [7], we assume that the cloud server is honest-but-curious. That is, the cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes [8], but will try to learn the content of the stored data and the identities of cloud users. AA Manager for group takes charge of system parameters generation, user registration, user revocation and revealing the real identity of a dispute data owner. Inthe given example, the AA manager is acted by the administrator of an organization. Therefore, we assume that the AA manager is fully trusted by the other parties. Group Members are a set of registered users that will store their private data into the cloud server and share them with others in the group. In my example, each group has members. Note that, the group membership is dynamically changed, due to the member resignation and new member participation in an organization.



III. LITERATURE SURVEY

D. Boneh et al.[1] focused on a Hierarchical Identity Based Encryption (HIBE) system where the ciphertext consists of just three group elements and decryption requires only two bilinear map computations, regardless of the hierarchy depth. Encryption is as efficient as in other HIBE systems. They prove that the scheme is selective-ID secure in the standard model and fully secure in the random oracle model. The system has a number of applications: it gives very efficient forward secure public key and identity based cryptosystems (with short ciphertexts), it converts the NNL broadcast encryption system into an efficient public key broadcast system, and it provides an efficient mechanism for encrypting to the future. The system also supports limited delegation where users can be given restricted private keys that only allow delegation to bounded depth. The HIBE system can be modified to support sublinear size private keys at the cost of some ciphertext expansion.

A.Fiat et al.[2] proposed a system on multicast communication framework, various types of security threat occurs. As a result construction of secure group communication that protects users from intrusion and eavesdropping are very important. In this paper, They propose an efficient key distribution method for a secure group communication over multicast communication framework. In this method, They use IP multicast mechanism to shortest rekeying time to minimize adverse effect on communication. In addition, They introduce proxy mechanism for replies from group members to the group manager to reduce traffic generated by rekeying. They define a new type of batching technique for rekeying in which new key is generated for both leaving and joining member. The rekeying assumption waits for 30 sec so that number time's key generation will be reduced.

S. Kamara et al.[3] proposed a security for customers to store and share their sensitive data in the cryptographic cloud storage. It provides a basic encryption and decryption for providing the security. HoIver, the revocation operation is a sure performance killer in the cryptographic access control system. To optimize the revocation procedure, they present a new efficient revocation scheme which is efficient, secure, and unassisted. In this scheme, the original data are first divided into a number of slices, and then published to the cloud storage. When a revocation occurs, the data owner needs only to retrieve one slice, and re-encrypt and re-publish it. Thus, the revocation process is accelerated by affecting only one slice instead of the whole data. They have applied the efficient revocation scheme to the cipher text-policy attribute-based encryption based cryptographic cloud storage. The security analysis shows that the scheme is computationally secure.

E. Goh et al.[4] presented a SiRiUS, a secure file system designed to be layered over insecure network and P2P file systems such as NFS, CIFS, Ocean Store, and Yahoo! Briefcase. SiRiUS assumes the network storage is untrusted and provides its own read-write cryptographic access control for file level sharing. Key management and revocation is simple with minimal out-of-band communication. File system freshness guarantees are supported by SiRiUS using hash tree constructions. SiRiUS contains a novel method of performing file random access in a cryptographic file system without the use of a block server. Extensions to SiRiUS include large scale group sharing using the NNL key revocation construction. Our implementation of SiRiUS performs Ill relative to the underlying file system despite using cryptographic operations. SiRiUS contains a novel method of performing file random access in a cryptographic file system without the use of a block server. Using cryptographic operations implementation of Sirius also possible. It only uses the own read write cryptographic access control. File level sharing are only done by using cryptographic access.

IV. REALATED WORK

To achieve secure data sharing for dynamic groups in the cloud, we expect to combine the group signature and dynamic broadcast encryption techniques. Specially, thegroup signature scheme enables users to anonymously usethe cloud resources, and the dynamic broadcast encryption technique

allows data owners to securely share their data files with others including new joining users. Unfortunately, each user has to compute revocation parameters to protect the confidentiality from the revoked users in the dynamic broadcast encryption scheme, which results in that both the computation overhead of the encryption and the size of the ciphertext increase with the number of revoked users. Thus, the heavy overhead and large ciphertext size may hinder the adoption of the broadcast encryption scheme to capacity-limited users. To tackle this challenging issue, we let the group manager compute the revocation parameters and make the result public available by migrating them into the cloud. Such a design can significantly reduce the computation overhead of users to encrypt files and the ciphertext size. Specially, the computation overhead of users for encryptionoperations and the ciphertext size are constant andindependent of the revocation users.

1. Group Creation Groups are creating by admin. A company allows its staffs in the same group or department to store and share files in the cloud. Any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud, which is defined as the multiple-owner manner.

2. User Registration For the registration of user i with identity IDi, the group manager randomly selects a number and characters for generate random key. Then, the group manager adds into the group user list, which will be used in the traceability phase. After the registration, user i obtains a private key, which will be used for group signature generation and file decryption.

3. Group Access Control When a data dispute occurs, the tracing operation is performed by the group manager to identify the real identity of the data owner. The employed group signature scheme can be regarded as a variant of the short group signature, which inherits the inherent unforgeability property, anonymous authentication, and tracking capability. The requirement of access control is twofold. First, group members are able to use the cloud resource for data operations. Second, unauthorized users cannot access the cloud resource at any time, and revoked users will be incapable of using the cloud again once they are revoked.

4. File Deletion File stored in the cloud can be deleted by either the group manager or the data owner (i.e., the member who uploaded the file into the server). To delete a file ID data, the group manager computes a signature ID data and sends the signature along with ID data to the cloud.

5. Revoke User User revocation is performed by the group manager via a public available revocation list RL, based on which group members can encrypt their data files and ensure the confidentiality against the revoked users. The admin can only have permission for revoke user and remove revocation. C.User Or Group Member Group members are a set of registered users that will store their private data into the cloud server and share them with others in the group.

1. File Upload To store and share a data file in the cloud, a group member checks the revocation list and verify the group signature. First, checking whether the marked date is fresh. Second, verifying the contained signature. Uploading the data into the cloud server and adding the ID data into the local shared data list maintained by the manager. On receiving the data, the cloud first to check its validity. It returns true, the group signature is valid; otherwise, the cloud stops the data. In addition, if several users have been revoked by the group manager, the cloud also performs revocation verification, the data file will be stored in the cloud after successful group signature and revocation verifications.

2. File Download Signature and Key Verification In general, a group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. Besides, the designated group manager can reveal the identity of the signature‟s originator when a dispute occurs, which is denoted as traceability.

3. OTP (One Time Password) OTPs avoid a number of shortcomings that are associated with traditional passwords. The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks.

V. CONCLUSION

In this paper, we design a secure anti-collusion data sharing scheme for dynamic groups in the cloud. In our scheme, the user scan securely obtain their private keys from group manager Certificate Authorities and secure communication channels. Also, our scheme is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated. Moreover, our scheme can achieve secure user revocation, the revoked users can not be able to get the original data files once they are revoked even if they conspire with the untrusted cloud.

REFERENCES

[1] X.Liu,B.Wang,Y.Zhang, and J.Yan,”Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud,”IEEE Computer Society,vol. 24,no. 6,June. 2013.

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

[3] G.Ateniese, R. Burns, R.urtmola, J.Herring, L. Kissner, Z. Peterson, and D.Song, “Deduplication in cloud storage using side channels in cloud services,” Oct 2008.

[4] 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.

[5] K. D. Bowers, A. Juels, and A. Oprea, ”Hail: A high-availability and integrity layer for cloud storage,” in Proc. Of CCS‟09, 2009, pp. 187-198.

[6] A. Fiat and M. Naor, “Broadcast Encryption,” Proc. Int‟lCryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.

[7] 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 .

[8] 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.

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