ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
DIIF 0.876

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 8, AUGUST 2015, PP 475-480

A Secure Multi-Owner Data Sharing Scheme for Dynamic Group in Public Cloud

1Allam Jyothi, [2] G.Somasekhar, [3]Dr S.Prem Kumar

[1](M.Tech), CSE, Assistant professor Department of Computer Science and Engineering

[2]Assistant Professor, Department of Computer Science and Engineering

[3]Professor & HOD, Department of computer science and engineering,

G.Pullaiah College of Engineering and Technology, Kurnool, Andhra Pradesh, India.

Abstract:

In cloud computing outsourcing group resource among cloud users is a major challenge, so cloud computing provides a low-cost and well-organized solution. Due to frequent change of membership, sharing data in a multi-owner manner to an untrusted cloud is still its challenging issue. In this paper we proposed a secure multi-owner data sharing scheme for dynamic group in public cloud. By providing AES encryption with convergent key while uploading the data, any cloud user can securely share data with others. Meanwhile, the storage overhead and encryption computation cost of the scheme are independent with the number of revoked users. In addition, I analyze the security of this scheme with rigorous proofs. One-Time Password is one of the easiest and most popular forms of authentication that can be used for securing access to accounts. One-Time Passwords are often referred to as secure and stronger forms of authentication in multi-owner manner. Extensive security and performance analysis shows that our proposed scheme is highly efficient and satisfies the security requirements for public cloud based secure group sharing.

Keywords: Cloud computing, Broadcast Encryption, Convergent Key Encryption, One Time password.

———————————— ◆ ————————————

1. INTRODUCTION

Cloud computing is Internet ("cloud") based development and use of computer technology ("computing"). It is a style of computing in which dynamically scalable and often virtualization resources are provided as a service over the internet. 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. First, identity privacy is one of the most significant obstacles for the wide deployment of cloud computing. Without the guarantee of identity privacy, users may be unwilling to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers. On the other hand, unconditional identity privacy may incur the abuse of privacy. For example, a misbehaved staff can deceive others in the company by sharing false files without being traceable. Therefore, traceability, which enables the group manager (e.g., a company manager) to reveal the real identity of a user, is also highly desirable. Second, it is highly recommended that 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 manners.

Compared with the single-owner manner [3], where only the group manager can store and modify data in the cloud, the multiple-owner manner is more flexible in practical applications. More concretely, each user in the group is able to not only read data, but also modify his/her part of data in the entire data file shared by the company. Last but not least, groups are normally dynamic in practice, e.g., new staff participation and current employee revocation in a company. The changes of membership make secure data sharing extremely difficult. On one hand, the anonymous system challenges new granted users to learn the content of data files stored before their participation, because it is impossible for new granted users to contact with anonymous data owners, and obtain the corresponding decryption keys. On the other hand, an efficient membership revocation mechanism without updating the secret keys of the remaining users is also

desired to minimize the complexity of key management. Several security schemes for data sharing untrusted servers have been proposed [4], [5], [6]. In these approaches, data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys.

The main issue in the public cloud is data sharing. So we are using many techniques to support the secure data sharing. Some of the techniques are certificate less encryption, functional proxy re-encryption; privacy preserving policy based content sharing, proxy provable data procession and so on. Fig 1 indicates the public cloud architecture

II.RELATED WORK

A. Cryptographic Cloud Storage:

S. Kamara et al.[9] 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 reencrypt 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.

B. Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing

S. Yu et al.[17] focused on many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. The problem of simultaneously achieving fine-grained, scalability, and data confidentiality of access control actually still remains unresolved. This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents. They achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. They proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability.

C. Ciphertext-Policy Attribute-Based Encryption:

an Expressive, Efficient, and Provably Secure Realization B. Waters et al.[16] proposed the character of low maintenance, cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent change of the membership. In this paper, they propose a secure multi- owner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. In addition, they analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments.

D. Sirius: Securing Remote Untrusted Storage

E. Goh et al.[7] 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.

E. Broadcast Encryption

A.Fiat et al.[6] 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.

III.SYSTEM MODEL

We consider a cloud computing architecture by combining with an example that a company uses a cloud to enable its staffs in the same group or department to share files. The system model consists of three different entities: the cloud, a group manager (i.e., the company manager), and a large number of group members (i.e., the staffs), and Group administrator (one of the Group member).

Cloud is operated by CSPs and provides priced abundant storage services. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users" trusted domain. Similar to [3], [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 [17], [18], but will try to learn the content of the stored data and the identities of cloud users. Group manager takes charge of system parameters generation, user registration, user revocation, and revealing the real identity of a dispute data owner. In the given example, the group manager is acted by the administrator of the company. Therefore, we assume that the group 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 our example, the staffs play the role of group members. Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company.

Due to overload of the group manager, he can give specific privileges to the one of the group member acting as Group administrator, he will functioning key assignment for new users and managing their group operations behalf of group manager. Here group admin may have revoked, group member may have revoked but group member can't revoke operations.

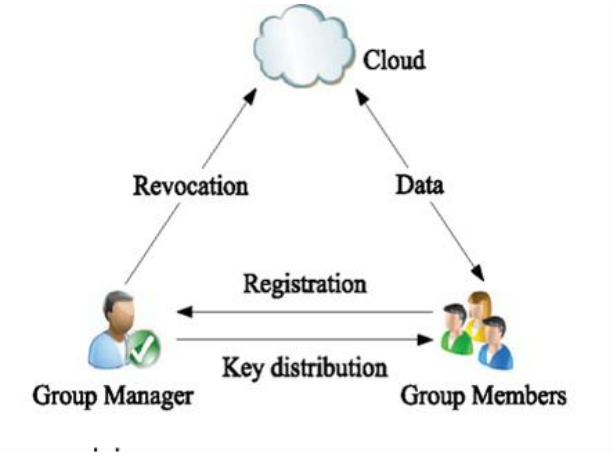

Fig 1. Presented System

A. Design Goals

In this section, we describe the main design goals of the proposed scheme including access control, data confidentiality, anonymity and traceability, and efficiency as follows:

Access control: The requirement of access control is in cases. First case, group members are able to use the cloud resource for data operations. Second case, 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.

Data confidentiality: Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of the stored data. An important and challenging issue for data confidentiality is to maintain its availability for dynamic groups. Specifically, new users should decrypt the data stored in the cloud before their participation, and revoked users are unable to decrypt the data moved into the cloud after the revocation.

Anonymity and traceability: Anonymity guarantees that group members can access the cloud without revealing the real identity. Although anonymity represents an effective protection for user identity, it also poses a potential inside attack risk to the system. For example, an inside attacker may store and share a mendacious information to derive substantial benefit. Thus, to tackle the inside attack, the group manager should have the ability to reveal the real identities of data owners.

Efficiency: The efficiency is defined as follows: Any group member can store and share data files with others in the group by the cloud. User revocation can be achieved without involving the remaining users. That is, the remaining users do not need to update their private keys or re-encryption operations. New granted users can learn all the content data files stored before his participation without contacting with the data owner.

IV. PROPOSED SYSTEM

A. Overview

To achieve secure data sharing for dynamic groups in the cloud, we expect to combine the group signature and Convergent key encryption techniques. Specially, the group signature scheme enables users to anonymously use the cloud resources, and the Convergent key encryption techniques 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 Convergent key encryption techniques, 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 encryption operations and the ciphertext size is constant and independent of the revocation users. Secure environments protect their resources against unauthorized access by enforcing access control mechanisms. So when increasing security is an issue text based passwords are not enough to counter such problems. Using the instant messaging service available in internet, user will obtain the One Time Password (OTP) after image authentication. This OTP then can be used by user to access their personal accounts. In this paper one time password to achieve high level of security in authenticating the user over the internet.

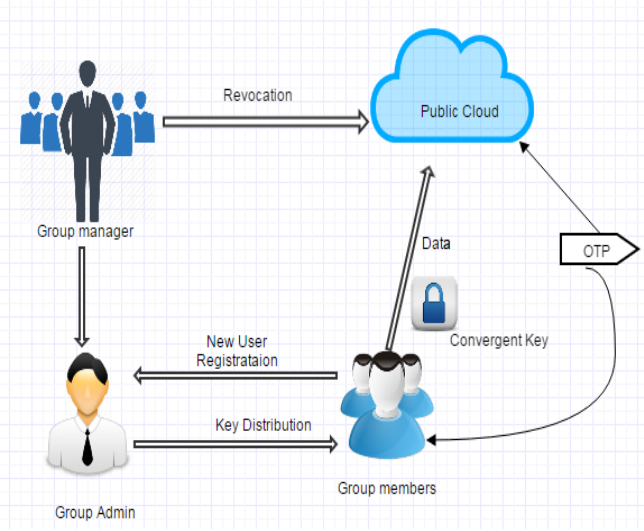

Fig 2. Proposed System Architecture

B. Group manager

1. **Group Creation** Groups are creating by manager. 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.

C. Group Admin

1. Group member joining

When a group member (Staff Member) joins, he/she sends a joining request to one group administrator (taking GAj for example). GAj handles this joining event as a sponsor. After verifying the new joining group member's legitimacy, GAj processes as follows:

GAj tries to find a leaf node which is mandated by one of the group administrators: If so, the found node is set as the associated one of the new joining group member. If not, GAj finds the leaf node with the smallest depth in the tree structure, and splits this node to a parent node and two children nodes. The left child is for existing group member associated to the found leaf node and the right one is for the new joining group member. Then, the new joining group member's process is as follows: Randomly select a security key. ◦ Get the blinded keys of all sibling nodes of every node in the path from his/her associated node to the root node from Cloud Servers. ◦ Compute new security keys and blinded keys of each node in the path from his/her associated node to the root node. ◦ set the versions of his/her associated node and its parent node to "0". Add 1 to the version of each of the other internal nodes in this path. ◦ Send all the blinded keys from his/her associated node to the root node in this path to the GAj in an authentication tunnel. Finally For the registration of user i with identity IDi, the group admin 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 user uses convergent key for encryption and file decryption.

2. Group Access Control When a data dispute occurs, the tracing operation is performed by the group admin 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.

3. 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.

4. Revoke 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.

D.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 Convergent Key to the local shared data list maintained by the group admin. 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 admin 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.

This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will be no longer valid. On the downside, OTPs are difficult for human beings to memorize.

OTP can be used to authenticate a user in a system via an authentication server. Also, if some more steps are carried out (the server calculates subsequent OTP value and sends/displays it to the user who checks it against subsequent OTP value calculated by his token), the user can also authenticate the validation server.

Generation of OTP Value

Step 1: Generate the HMAC-SHA value Let HMK = HMAC-SHA(Key, T) // HMK is a 20-byte string

Step 2: Generate a hex code of the HMK. HexHMK=ToHex (HMK)

Step 3: Extract the 8-digit OTP value from the string

OTP = Truncate (HexHMK) the Truncate function in Step 3 does the dynamic truncation and reduces the OTP to 8-digit.

4. AES Encryption

The input 16 byte Plain text can be converted into 4×4 square matrix. The AES Encryption consists of four different stages they are

Substitute Bytes: Uses an S-box to perform a byte-by-byte substitution of the block

Shift Rows: A Simple Permutation

Mix Columns: A substitution that makes use of arithmetic overGF(28)

Add Round Key: A Simple Bitwise XOR of the current block with the portion of the expanded key

5. AES Decryption

The Decryption algorithm makes use of the key in the reverse order. However, the decryption algorithm is not identical to the encryption algorithm

V.CONCLUSSION

In this paper we proposed a dynamic secure group sharing framework in public cloud computing environment. In our proposed scheme, the administration privilege can be approved to some specific group members based on Convergent Key scheme; all the sharing files are secured stored in Cloud Servers and the entire session key are protected. We use Cloud Servers' aid based OTP to dynamical updating group key pair when there're group members leaving or joining the group, our scheme can still do well which can delegate most of computing overhead to Cloud Servers without disclosing any security information. From the security and performance analysis, the proposed scheme can achieve the design goal, and keep a lower computational complexity and communication overhead in each group members' side.

REFERENCES:

[1] L. Backstrom, D. Huttenlocher, J. Kleinberg, and X. Lan, "Group formation in large social networks: membership, growth, and evolution," in ACM SIGKDD2006: Proc. 12th international conference on Knowledge discovery and data mining. ACM, 2006, pp. 44–54.

[2] A. T. Sherman and D. A. McGrew, "Key establishment in large dynamic groups using one-way function trees," IEEE Transactions on Software Engineering, vol. 29, no. 5, pp. 444–458, 2003.

[3] C. K. Wong, M. Gouda, and S. S. Lam, “Secure group communications using key graphs,” IEEE-ACM Transactions on Networking, vol. 8, no. 1, pp. 16–30, 2000.

[4] M. Steiner, G. Tsudik, and M. Waidner, “Key agreement in dynamic peer groups,” IEEE Transactions on Parallel and Distributed Systems, vol. 11, no. 8, pp. 769–780, 2000.

[5] Y. Kim, A. Perrig, and G. Tsudik, “Group key agreement efficient in communication,” IEEE Transactions on Computers, vol. 53, no. 7, pp. 905–921, 2004.

[6] W. Yu, Y. Sun, and K. R. Liu, “Optimizing the rekeying cost for contributory group key agreement schemes,” IEEE Transactions on Dependable and Secure Computing, vol. 4, no. 3, pp. 228–242, 2007.

[7] W. Trappe, Y. Wang, and K. R. Liu, “Resource-aware conference key establishment for heterogeneous networks,” IEEE-ACM Transactions on Networking, vol. 13, no. 1, pp. 134–146, 2005.

[8] Y. Kim, A. Perrig, and G. Tsudik, “Tree-based group key agreement,” ACM Transactions on Information and System Security (TISSEC), vol. 7, no. 1, pp. 60–96, 2004.

[9] V.Sathana, J.Shanthini” Enhanced Security System for Dynamic Group in Cloud” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 3, March 2014