Volume 2, Issue 11, November-2015, pp. 775-779 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

A Survey on Dynamic Secure group Data Sharing framework among Public Cloud

[1]Pathan Jilani,[2]Sayeed Yasin

[1](M.Tech) IT, Nimra College of Engineering & Technology

[2]Associate Professor & HOD, Dept of CSE, Nimra College of Engineering & Technology.

Abstract: - In cloud computing outsourcing, cluster plus among cloud shoppers could be a noteworthy check, therefore cloud computing provides a token effort and everyone around sorted out the arrangement. Thanks to incessant modification of participation, sharing data Associate in Nursing exceedingly in a very multi-owner manner to an untrusted cloud continues to be its testing issue. During this paper, we have a tendency to project a protected multi-owner data sharing arrange for a dynamic cluster in folks, in general, cloud. By furnishing AES cryptography with convergent key whereas transferring the knowledge, any cloud shopper will safely impart data to others. Within the in the meantime, the capability overhead and cryptography calculation expense of the arrange area unit free with the amount of unacknowledged shoppers. Also, I break down the protection of this arrange with thorough confirmations. One-Time Secret word is one in every of the only and most well-known sorts of confirmation which will be utilized for securing access to accounts. One-Time Passwords area unit of times alluded to as secure and additional grounded sorts of confirmation in an exceedingly multi-owner manner. Broad security and execution examination demonstrates that our projected arrange is deeply productive and fulfills the protection requirements for open cloud-based secure cluster sharing.

Keywords – Cloud computing, broadcast encryption.

1. INTRODUCTION

Cloud computing is net ("cloud") based mostly development and use of technology ("computing"). It's a method of computing within which dynamically scalable and sometimes virtualization resources are provided as a service over the net. One amongst the foremost basic services offered by cloud suppliers is information storage. Allow us to contemplate a sensible information application. A corporation permits its staffs within the same cluster or department to store and share files within the cloud. However, it additionally poses a big risk to the confidentiality of these keep files. Specifically, the cloud servers managed by cloud suppliers don't seem to be absolutely trusty by users whereas the information files keep within the cloud could also be sensitive and confidential, like business plans. To preserve information privacy, a basic answer is to write information files, so transfer the encrypted information into the cloud. First, identity privacy is one amongst the foremost vital obstacles for the wide preparation of cloud computing. While not the guarantee of identity privacy, users could also be unwilling to hitch in cloud computing systems as a result of their real identities may well be simply disclosed to cloud suppliers and attackers. On the opposite hand, unconditional identity privacy could incur the abuse of privacy. For instance, misbehaved employees will deceive others within the company by sharing false files while not being traceable. Therefore, traceability, that allows the cluster manager (e.g., a corporation manager) to reveal the $64000 identity of a user, is additionally extremely fascinating. Second, it's extremely suggested that any member during a cluster ought to be ready 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.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.

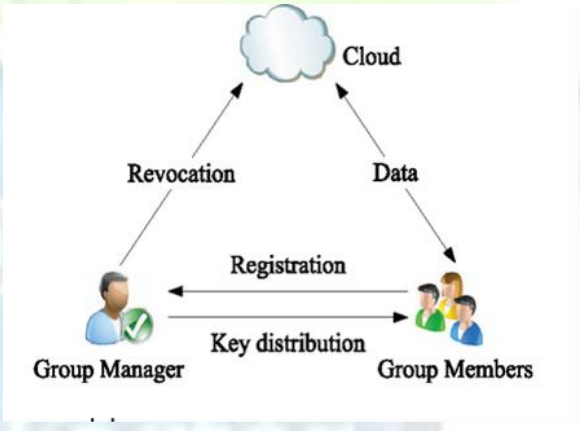

Fig 1. Presented System

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.

III. PROPOSED SYSTEM

A. Overview

To accomplish secure data sharing for dynamic groups in the cloud, we hope to join the group signature and Convergent Key encryption procedures. Particularly, the group mark plan empowers clients to namelessly utilize the cloud assets, and the Merged key encryption procedures permit data owners to safely import their data documents to others including new joining clients. Lamentably, every client needs to register repudiation parameters to shield the classification from the disavowed clients in the Convergent Key encryption procedures, which brings about that both the calculation overhead of the encryption and the span of the ciphertext increment with the quantity of renounced clients. Accordingly, the substantial overhead and vast ciphertext size may block the selection of the telecast encryption plan to limit constrained clients. To handle this testing issue, we let the group administrator register the renouncement parameters and make the subsequent open accessible by moving them into the cloud. Such a configuration can fundamentally lessen the calculation overhead of clients to scramble documents and the ciphertext size. Particularly, the calculation overhead of clients for encryption operations and the ciphertext size is consistent and free of the repudiation clients. Secure situations ensure their assets against unapproved access by authorizing access control components. So while expanding security is an issue content based passwords are insufficient to counter such issues. Utilizing the texting administration accessible in the web, a client will acquire the One Time Secret key (OTP) after picture verification. This OTP then can be utilized by a client to get to their own records. In this paper one-time secret key to accomplishing the abnormal state of security in authenticating the client over the web.

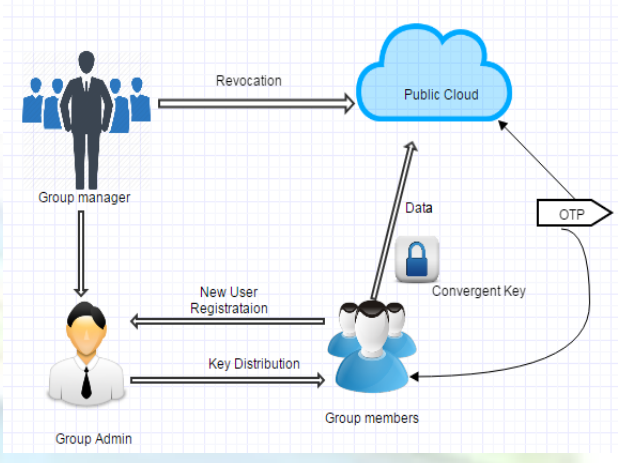

Fig 2. Proposed System Architecture

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 tend to plan a dynamic secure cluster sharing framework, in general, society cloud computing atmosphere. In our planned arrange, the organization profit is supported to some explicit cluster people in light-weight of focused Key Scheme; all the sharing documents square measure secured place away in Cloud Servers and also the whole session key square measure ensured. we tend to utilize Cloud Servers' guide primarily based OTP to high-powered upgrading cluster key try once they are cluster people effort or change of integrity the cluster, our arrange will in any case had best which may appoint the bulk of computing overhead to Cloud Servers while not unveiling any security knowledge. From the protection and execution investigation, the planned arrange will accomplish the made public objective, and keep a lower process many-sided nature and correspondence overhead in each cluster individuals' aspect.

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

