Volume 5, Issue 10, October-2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

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

[1]Kamepalli S L Prasanna, [2]Kotha Mohan Krishna
[1] (M.Tech) –CSE, Vasireddy Venkatadri Institute of Technology (VVIT), Andhra Pradesh, India
[2]Assistant Professor, Dept of CSE, Vasireddy Venkatadri Institute of Technology (VVIT), Nambur (V), Guntur (Dt.) Andhra Pradesh, India

Abstract: ***In cloud computing outsourcing gathering asset among cloud clients is a noteworthy test so cloud computing gives a minimal effort and very much sorted out arrangement. Because of incessant change of participation, sharing information in a multi-owner way to an untrusted cloud is still its testing issue. In this paper we proposed a safe multi-owner information sharing plan for element bunch in broad daylight cloud. By giving AES encryption merged key while transferring the information, any cloud client can safely impart information to others. In the interim, the capacity overhead and encryption calculation expense of the plan are autonomous with the quantity of revoked clients. What's more, I break down the security of this plan with thorough evidences. One-Time Secret key is one of the simplest and most prominent types of confirmation that can be utilized for securing access to accounts. One-Time Passwords are frequently alluded to as secure and more grounded types of verification in multi-owner way. Broad security and execution examination demonstrates that our proposed plan is exceedingly productive and fulfills the security prerequisites for open cloud based secure group sharing.***

Keywords: Cloud computing, broadcast Encryption, OTP, AES encryption.

I. INTRODUCTION

Cloud computing is Web ("cloud") based advancement and utilization of PC innovation ("computing"). It is a style of computing in which dynamically scalable and frequently virtualization assets are given as an administration over the web. A standout amongst the most crucial administrations offered by cloud suppliers is data stockpiling. Give us a chance to consider a reasonable data application. An organization permits its staffs in the same gathering or division to store and share files in the cloud. Then again, it additionally represents a critical danger to the classification of those put away files. In particular, the cloud servers oversaw by cloud suppliers are not completely trusted by clients while the data files put away in the cloud may be delicate and classified, for example, strategies for success. To protect data security, an essential arrangement is to encrypt data files, and afterward transfer the encrypted data into the cloud. To start with, character security is a standout amongst the most noteworthy snags for the wide arrangement of cloud computing. Without the surety of personality security, clients may be unwilling to join in cloud computing frameworks in light of the fact that their genuine characters could be effectively unveiled to cloud suppliers and aggressors. Then again, unrestricted personality security may bring about the misuse of protection. For instance, a got into mischief staff can delude others in the organization by sharing false files without being traceable. Accordingly, traceability, which empowers the gathering chief (e.g., an organization director) to uncover the genuine character of a client, is likewise exceptionally attractive. Second, it is profoundly suggested that any part in a gathering ought to have the capacity to completely appreciate the data putting away and sharing administrations gave by the cloud, which is characterized as the multiple owner behavior.

Contrasted and the single-owner way [3], where just the gathering supervisor can store and adjust data in the cloud, the multiple-owner way is more adaptable in down to earth applications. All the more solidly, every client in the gathering has the capacity perused data, as well as alter his/her a player in data in the whole data document shared by the organization. To wrap things up, gatherings are ordinarily changing by and by, e.g., new staff support and current representative renouncement in an organization. The progressions of enrollment make secure data sharing to a great degree troublesome. On one hand, the mysterious framework challenges new allowed clients to take in the substance of data files put away before their cooperation, on the grounds that it is inconceivable for new conceded clients to contact with unknown data owners, and acquire the comparing unscrambling keys. Then again, a productive participation disavowal component without redesigning the mystery keys of the remaining clients is likewise wanted to minimize the multifaceted nature of key administration. A few security plans for data sharing untrusted servers have been proposed [4], [5], and [6]. In these methodologies, data owners store the encrypted data files in untrusted stockpiling and disseminate the relating unscrambling keys just to approved clients. Along these lines, unapproved clients and in addition stockpiling servers can't take in the data's substance files in light of the fact that they have no learning of the decoding keys.

The principle issue in the general population cloud is data sharing. So we are utilizing numerous systems to bolster the protected data sharing. A methods' portion are declaration less encryption, useful intermediary re-encryption; protection saving strategy based substance sharing, intermediary provable data parade et cetera. Fig 1 indicates the public cloud architecture

II. RELATED WORK

A. Cryptographic Cloud Storage:

S. Kamara et al.[9] proposed a security for clients to store and share their touchy data in the cryptographic cloud stockpiling. It gives a fundamental encryption and decryption for giving the security. HoIver, the denial operation is a certain execution executioner in the cryptographic access control framework. To enhance the disavowal technique, they display another productive denial plan which is proficient, secure, and unassisted. In this plan, the first data are initially isolated into various cuts, and then distributed to the cloud stockpiling. At the point when a denial happens, the data owner needs just to recover one cut, and reencrypt and re-distribute it. Along these lines, the denial procedure is quickened by influencing one and only cut rather than the entire data. They have connected the effective repudiation plan to the figure content arrangement characteristic based encryption based cryptographic cloud stockpiling. The security investigation demonstrates that the plan is computationally secure.

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

S. Yu et al.[17] concentrated on numerous new difficulties for data security and access control when clients outsource delicate data for sharing on cloud servers, which are not inside of the same trusted space as data owners. To keep touchy client data private against untrusted servers, existing arrangements for the most part apply cryptographic techniques by unveiling data decryption keys just to approved clients. The issue of all the while accomplishing fine-grained, adaptability, and data confidentiality of access control entirely stays uncertain. This paper addresses this testing open issue by, on one hand, characterizing and implementing access arrangements in light of data traits, and, then again, permitting the data owner to appoint a large portion of the calculation errands included in fine-grained data access control to untrusted cloud servers without uncovering the hidden data substance. They accomplish this objective by abusing and interestingly joining strategies of characteristic based encryption (ABE), intermediary re-encryption, and sluggish re-encryption. They proposed plan additionally has notable properties of client access benefit confidentiality and client mystery key responsibility.

C. Sirius: Securing Remote Untrusted Storage

E. Goh et al.[7] presented a SiRiUS, a protected document framework intended to be layered over frail system and P2P record frameworks, for example, NFS, CIFS, Sea Store, and Yippee! Satchel. SiRiUS expect the system stockpiling is untrusted and gives its own particular read-compose cryptographic access control for document level sharing. Key administration and denial is basic with negligible out-of-band correspondence. Record framework freshness assurances are upheld by SiRiUS utilizing hash tree developments. SiRiUS contains a novel strategy for performing record random access in a cryptographic document framework without the utilization of a square server. Expansions to SiRiUS incorporate vast scale group sharing utilizing the NNL key denial development. Our execution of SiRiUS performs Sick in respect to the basic document framework regardless of utilizing cryptographic operations. SiRiUS contains a novel strategy for performing record random access in a cryptographic document framework without the utilization of a square server. Utilizing cryptographic operations usage of Sirius additionally conceivable. It just uses the own read compose cryptographic access control. Records level using so as to share are just done cryptographic access.

E. Broadcast Encryption

A.Fiat et al.[6] proposed a framework on multicast correspondence system, different sorts of security risk happens. Therefore development of secure group correspondence that shields clients from interruption and listening stealthily are critical. In this paper, they propose a productive key circulation system for a protected group correspondence over multicast correspondence structure. In this system, they utilize IP multicast instrument to most limited rekeying time to minimize unfavorable impact on correspondence. Also, they present intermediary instrument for answers from group individuals to the group manager to decrease activity produced by rekeying. They characterize another kind of bunching strategy for rekeying in which new key is created for both leaving and joining part. The rekeying presumption sits tight for 30 sec with the goal that number time's key era will be diminished.

III. SYSTEM MODEL

We consider a cloud combining so as to compute structural planning with a sample that an organization uses a cloud to empower its staffs in the same group or office to share files. The framework model comprises of three distinct substances: the cloud, a group manager (i.e., the organization manager), and an extensive number of group individuals (i.e., the staffs), and Group head (one of the Group part).

Cloud is worked by CSPs and gives valued bottomless stockpiling administrations. On the other hand, the cloud is not completely trusted by clients since the CSPs are liable to be outside of the cloud users‟ trusted space. Like [3], [7], we expect that the cloud server speaks the truth however inquisitive. That is, the cloud server won't noxiously erase or change client data because of the security of data evaluating plans [17], [18], yet will attempt to take in the substance of the put

away data and the characters of cloud clients. Group manager assumes responsibility of framework parameters era, client enlistment, client renouncement, and uncovering the genuine character of a debate data owner. In the given illustration, the group manager is acted by the organization's chairman. Along these lines, we accept that the group manager is completely trusted by alternate gatherings. Group individuals are an arrangement of enrolled clients that will store their private data into the cloud server and offer them with others in the group. In our case, the staffs assume the part of group individuals. Note that, the group enrollment is dynamically changed, because of the staff renunciation and new representative cooperation in the organization.

Because of over-burden of the group manager, he can give particular benefits to the group's one part going about as Group executive, he will working key task for new clients and dealing with their group operations sake of group manager. Here group administrator may have revoked, group part may have revoked yet group part can't repudiate operation.

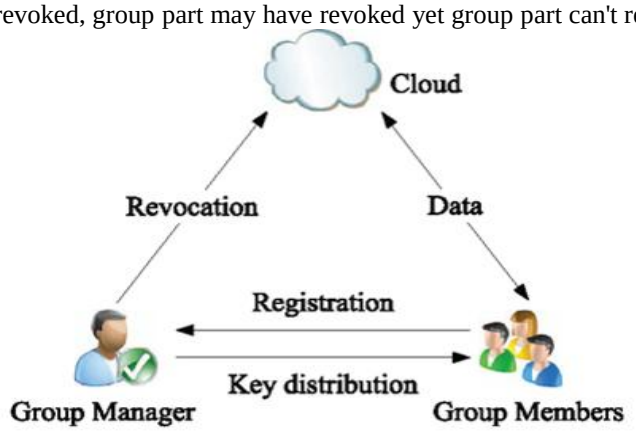

Fig 1. Presented System

A. Design Goals

In this area, we depict the principle plan objectives of the proposed plan including access control, data confidentiality, obscurity and traceability, and productivity as takes after:

Access control: The prerequisite of access control is in cases. To start with case, group individuals have the capacity to utilize the cloud asset for data operations. Second case, unapproved clients can't get to the cloud asset whenever, and revoked clients will be unequipped for utilizing the cloud again once they are revoked.

Data confidentiality: Data confidentiality obliges that unapproved clients including the cloud are unequipped for taking in the substance of the put away data. A vital and testing issue for data confidentiality is to keep up its accessibility for element groups. In particular, new clients ought to decrypt the data put away in the cloud before their support, and revoked clients are not able to decrypt the data moved into the cloud after the repudiation.

Anonymity and traceability: Anonymity ensures that group individuals can get to the cloud without uncovering the genuine personality. In spite of the fact that secrecy speaks to a compelling assurance for client character, it likewise represents a potential inside assault danger to the framework. For instance, an inside aggressor may store and share a duplicitous data to infer considerable advantage. In this way, to handle within assault, the group manager ought to be able to uncover the genuine personalities of data owners.

Efficiency: The proficiency is characterized as takes after: Any group part can store and impart data files to others in the group by the cloud. Client repudiation can be accomplished without including the remaining clients. That is, the remaining clients don't have to overhaul their private keys or re-encryption operations. New allowed clients can realize all the substance data files put away before his support without reaching 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.

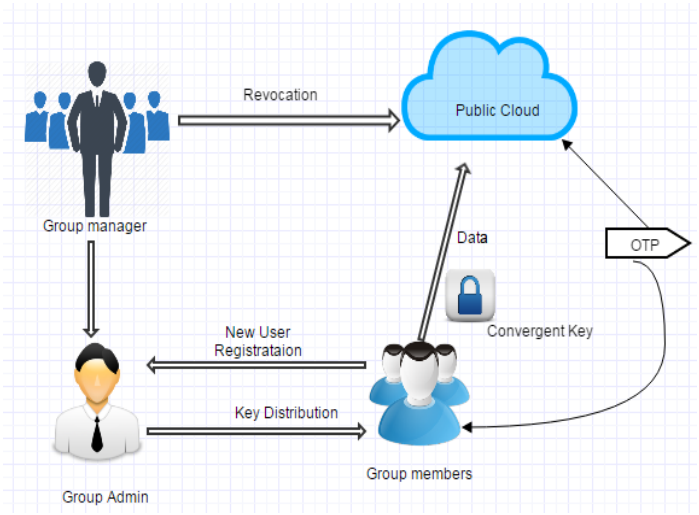

Fig 2. Proposed System Architecture

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] Kaiping Xue and Peilin Hong ,"A Dynamic Secure Group Sharing Framework in Public Cloud Computing", IEEE Transactions on Cloud Computing, vol:pp no:99, 2014.

[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.

[10] Allam Jyothi, G.Somasekhar And Dr S.Prem Kumar ,"A Secure Multi-Owner Data Sharing Scheme For Dynamic Group In Public Cloud." International Journal of Computer Engineering In Research Trends. Volume 2, Issue 8, August 2015, pp 475-480, Issn (Online): 2349-7084. www.ijcert.org.

[11] 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.

