Sharing Secure encrypt Data in the Cloud Computing for the Multiuser Groups

A.Sowjanya [1], Dr.K.Venkataramana[2]
[1]*Student, Dept. of MCA, KMM Institute of Post Graduate Studie, Tirupati,A.P*
[2]*Assistant Professor, Dept. of MCA, KMM Institute of Post Graduate Studies, Tirupati,A.P*

***Abstract*- Security is the main concern in the cloud computing environment. The usage of the cloud computing in increasing gradually, where the security is still lagging. we present a secure multi owner data sharing scheme for dynamic groups in the cloud computing. By leveraging on group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. In this propose a new model for Sharing Secure Data in the Cloud computing for the Multiuser Groups. In this one of the biggest concern with cloud data storage is that of data integrity verification at untreated servers. To preserve data privacy, the basic solution is to encrypt data files, and then upload the encrypted data into the cloud. To resolve this problem recently the best efficient method MONA presented for secured multi owner data sharing in however we identified some limitations in that same approach in terms of reliability and scalability. Hence in this paper we are further extending the basic MONA by adding the reliability and as well as improving the scalability by increasing the number of group managers dynamically.**

***Index Terms*- Cloud Computing, Data Sharing, Group Signature, Dynamic Groups, User Revocation, Access Control**

I. INTRODUCTION

Cloud computing is one of the greatest platforms which provide storage of data in very lesser cost and available for all time over the internet Cloud computing is Internet-based computing, whereby shared resources, software and information are provided to computers and devices on demand. In this several trends are opening up the era of Cloud Computing, which are an Internet-based development and use of computer technology. Cloud Computing means more than simply saving on Information Technology implementation costs. Cloud Computing offers enormous opportunity for new innovation, and even disruption of entire industries. So Cloud computing is the long dreamed vision of computing as a utility, where data owners can remotely store their data in the cloud to enjoy on-demand high-quality applications and services from a shared pool of configurable computing resources.

Cloud Computing is recognized as an alternative to traditional Information Technology (IT) due to its intrinsic resource-sharing and low-maintenance characteristics. In this cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud computing users with the help of powerful data centers. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures, and 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. 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 encrypting data files, and then uploads the encrypted data into the cloud.

Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following challenging issues. Many privacy techniques for data sharing on remote storage machines have been recommended. In these models, the data owners store the encrypted data on untreated remote storage. After that they will share the respective decryption keys with the authorized users. This prevent the cloud service providers and intruders to access the encrypted data, as they don't have the decrypting keys. However the new data owner

registration in the above said models reveals the identity of the new data owner to the others in the group. The new data owner has to take permission from other data owners in the group before generating a decrypting key. The proposed system identified the problems during multi owner data sharing and proposed an efficient protocols and cryptographic techniques for solving drawbacks in the traditional approach. In this it proposed an efficient and novel secure key protocol for group key generation and using these key data owners can encrypt the all files. Suppose new user register into group the user need not to contact the data owner during the downloading of files and data can be encrypted with AES before uploading the data in to the cloud.

II. LITERATURE SURVEY

Goh, H. Shacham, N. Modadugu, and D. Boneh [2] the use of SiRiUS is compelling in situations where users have no control over the file server (such as Yahoo! Briefcase or the P2P file storage provided by Farsite). They believe that SiRiUS is the most that can be done to secure an existing network file system without changing the file server or file system protocol. 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.

B. Wang, B. Li, and H. Li, [3] in this paper, we propose Knox, a privacy-preserving auditing scheme for shared data with large groups in the cloud. They utilize group signatures to compute verification information on shared data, so that the TPA is able to audit the correctness of shared data, but cannot reveal the identity o f the signer on each block. With the group manager's private key, the original user can efficiently add new users to the group and disclose the identities of signers on all blocks. The efficiency of Knox is not affected by the number of users in the group.

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 [9] the data centers hardware and software is what we will call a cloud. When a cloud is made available in a pay-as-you-go manner to the general public, they call it a public cloud; the service being sold is utility computing. They use the term private cloud to refer to internal data centers of a business or other organization, not made available to the general public, when they are large enough to benefit from the advantages of cloud computing that we discuss here. Thus, cloud computing is the sum of SaaS and utility computing, but does not include small or medium-sized data centers, even if these rely on virtualization for management. People can be users or providers of SaaS, or users or providers of utility computing. They focus on SaaS providers (cloud users) cloud providers, which have received less attention than SaaS users.

S. Kamara and K. Lauter [4] in this paper consider the problem of building a secure cloud storage service on top of a public cloud infrastructure where the service provider is not completely trusted by the customer. They describe, at a high level, several architectures that combine recent and non-standard cryptographic primitives in order to achieve the goal. Survey the benefits such architecture would provide to both customers and service providers and give an overview of recent advances in cryptography motivated specifically by cloud storage.

A. Fiat and M. Naor [6] they introduce new theoretical measures for the qualitative and quantitative assessment of encryption schemes designed for broadcast transmissions. The goal is to allow a central broadcast site to broadcast secure transmissions to an arbitrary set of recipients while minimizing key management related transmissions.
They present several schemes that allow centers to broadcast a secret to any subset of privileged users out of a universe of size so that coalitions of users not in the privileged set cannot learn the secret.

V. Goyal, O. Pandey, A. Sahai, and B. Waters [6] they develop a new cryptosystem for One-grained sharing of encrypted data that call Key-Policy Attribute-Based Encryption (KP-ABE). In cryptosystem, cipher texts are labelled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. They demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption. Our construction supports delegation of private keys which subsumes

Hierarchical Identity-Based Encryption (HIBE). The data owner uses a random key to encrypt a file, where the random key is further encrypted with a set of attributes using KP-ABE. Then, the group manager assigns an access structure and the corresponding secret key to authorized users, such that a user can only decrypt a ciphertext if and only if the data file attributes satisfy the access structure. To achieve user revocation, the manager delegates tasks of data file reencryption and user secret key update to cloud servers. However, the single owner manner may hinder the implementation of applications with the scenario, where any member in a group should be allowed to store and share data files with others.

By Observing all this analysis we have a greater challenging issue that is how we can securely share data with the others by the multiple-owner manner for the dynamic groups in the un trusted cloud along with preserving identity privacy. Now in this paper, we are surveying new protocol MONA, for secure data sharing in the cloud computing. The MONA offers some unique features when compared with the others. The unique features in a more elaborated way are as follows:

- Any group member can share data files with others and can also store the data files in the cloud.
- In this the number of revoked users is independent with the complexity of encryption and also the size of cipher texts.
- There is no need of updating the private keys of the remaining users whenever the user revocation occurs
- The new users can directly access the files that are stored n the cloud without their participation.

III .SYSTEM DESIG

Existing System

To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task.

The 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. However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively.

In the literature study we have seen many methods for secure data sharing in cloud computing, however most methods failed to achieve the efficient as well as secure method for data sharing for groups. To provide the best solutions for the problems imposed by existing methods, recently the new method was presented called MONA [1]. This approach presents the design of secure data sharing scheme, Mona, for dynamic groups in an untrusted cloud. In Mona, a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, Mona supports efficient user revocation and new user joining. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant. Therefore practically in all cases MONA outperforms the existing methods.

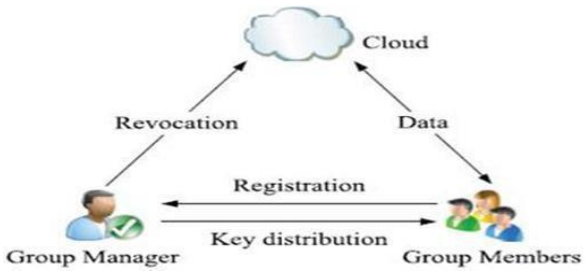


Fig 1. Existing System Model

Revocation List

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 revocation list is characterized by a series of time stamps (t1 < t2 <,…, tr). Let IDgroup denote the group identity. The tuple (Ai, xi, ti) represents that user i with the partial private key is revoked at time ti. P1, P2 …, Pr and Zr are calculated by the group manager with the private secret as follows:

here x1=y1, x2=y2 and xr=yr.

$$\begin{cases} P_1 = \frac{1}{\gamma + x_1} \cdot P \in G_1 \\ P_2 = \frac{1}{(\gamma + x_1)(\gamma + x_2)} \cdot P \in G_1 \\ P_r = \frac{1}{(\gamma + x_1)(\gamma + x_2) \cdots (\gamma + x_r)} \cdot P \in G_1 \\ Z_r = Z^{\frac{1}{(\gamma + x_1)(\gamma + x_2) \cdots (\gamma + x_r)}} \in G_2. \end{cases}$$

Disadvantage

However as per reliability and scalability concern this method needs to be workout further as if the group manager stop working due to large number of requests coming from different groups of owners, then entire security system of MONA will fail. In revocation list the time given for each user is fixed so after the time expires user cannot access the data until group manager update the revocation list and give it to the cloud.

Design Goals

We describe the main design goals of the proposed system including access control, data confidentiality, anonymity and traceability, and efficiency as follows:

Access control: First, authorized group members are able to access the cloud data. Second, unauthorized users cannot access the cloud data at any time, and revoked users will not be capable of accessing the cloud once they are revoked.

Data confidentiality: Data confidentiality requires that unauthorized users are not capable to access the content of the stored data. An important and challenging issue for data confidentiality for dynamic groups. Specifically, new users should access the data stored in the cloud before their participation, and revoked users are unable to access the data after the revocation. Data owner will store the data on the cloud and share among the group members and data owner will modify the data and delete the data in the cloud.

Anonymity and traceability: Anonymity guarantees that group members can access the cloud without revealing the real identity. Although anonymity is an effective protection for users identity, it also poses a potential inside attack risk to the system. For example, an inside attacker may store and share a malicious information to get the important information. Thus, to remove the inside attack, the group manager should have the ability to verify the real identities or members of data owners. If the one group member access the data and delete or modify the data by other group members data can be easily traceable in the cloud.

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 is achieved by without involving the remaining users. The remaining users do not need to update their private keys or re encryption operations. New group member can access all the content data files stored on cloud before his participation without contacting with the data owner.

Proposed System

To achieve the reliable and scalable in MONA, in this paper we are surveying the new framework for MONA. In this method we are further presenting how we are managing the risks like failure of group manager by increasing the number of backup group manager, hanging of group manager in case number of requests more by sharing the workload in multiple group managers.

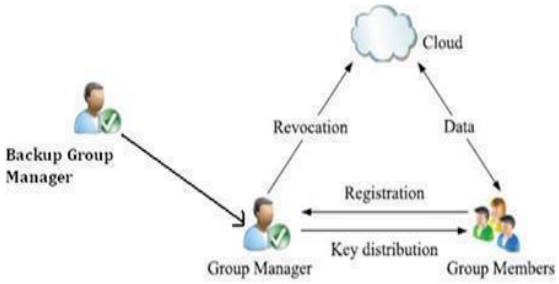


Fig 2. Proposed System Model

This method claims required efficiency, scalability and most importantly reliability.To overcome the disadvantage of existing system MONA, in the proposed MONA is if the group manager stop working due to large number of requests coming from different groups of owners, then backup group manager will remain available. Here user gets extra time for accessing data after the time out by sending request to the cloud.

Scheme Description

This section describes system, initialization, user registration, user revocation, file generation, file deletion and file access.

System Initialization

The group manager takes charge of system initialization as follows:

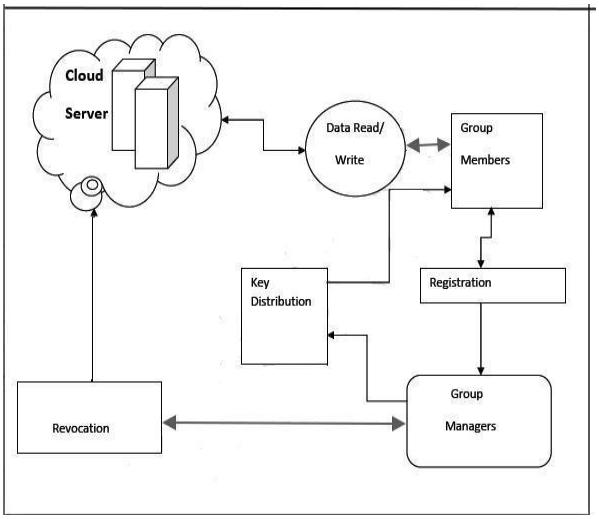
Generating a bilinear map group system S=(q, G1, G2,e(.,.)).
The system parameters including (S, P, H, H0 ,H1 ,H2, U, V , W , Y , Z, f, f1, Enc()), where f is a one-way hash function: {0,1}* —> Z*q ; f1 is hash function: {0,1}* —> G1; and Enck() is a secure symmetric encryption algorithm with secret key k.

User Registration
For the registration of user i with identity IDi, the group manager randomly selects a number xi belong to Z*q and computes Ai, Bi.
Then, the group manager adds (Ai, xi, IDi) into the group user list, which will be used in the traceability phase. After the registration, user i obtains a private key (xi, Ai, Bi), which will be used for group signature generation and file decryption.

Revocation List
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 list is characterized by time stamp t1,t2,…tr. In the proposed system once the user time stamp is over he need not wait for the group manager to update the time stamp or revocation list, the user can immediately send request for extra time for accessing the data to the cloud. Then the cloud will send that request to the group manager who can give permission

File Generation
To store and share a data file in the cloud, a group member performs the following operations:
Getting the revocation list from the cloud. In this step, the member sends the group identity IDgroup as a request to the cloud. Then, the cloud responds the revocation list RL to the member. Verifying the validity of the received revocation list. First, checking whether the marked date is fresh or not. Second, verifying the contained signature sig(RL) by the equation e(W, f1 (RL)) = e(P, sig(RL)). If the revocation list is invalid, the data owner stops this scheme. Encrypting the data file M. Selecting a random number T and computing f T. The hash value will be used for data file deletion operation. In addition, the data owner adds (ID data, T) into his local storage. Constructing the uploaded data file as shown in Table 2, where t data denotes the current time on the member, and a group signature on (ID data, C1, C2, C, f(T); t data) computed by the data owner through private key (A, x).

Mona Architecture



The architecture model consists of three main different entities: The Cloud Server, Group Manager (admin) and a large number of Group Members.

- Cloud Server: Cloud is operated by cloud service providers and provides priced abundant storage services.
- Group Manager: Group Manager takes the charge of system parameters like user registration, user revocation, secret key generation.
- Group Members: Group members are the set of registered users that will store their private data into the cloud server and can download it and share the data with others in the group

Cloud Server: Cloud is the large repository of resources. Cloud is responsible for storing all user's data and granting access to the file within a group to other group members based on publically available revocation list which is maintained by group manager. We assume that the cloud server is honest but curious. That is, the cloud server will not maliciously delete or modify user data, but will try to learn the content of the stored data.

Group Manager**:** 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 manager perform various operations such as system parameters generation, user registration, group creation, assign group signature, generation of private key using bilinear mapping and assign to the requested user, maintain revocation list and migrate this list into cloud for public use, and traceability.

Group Members:

Group members are a collection of registered users that will store their private data into the cloud server and share them with others in the group.

Algorithms Used:-

Signature Generation - The group signature and file key generation can be done by using the Triple DES encryption process.

Signature Verification – The verification of group signature key and file key's with the Triple DES decryption process.

Revocation Verification - To check the user revocation which is used for the verification of user's list.

Simulation

To Study the performance we simulate MONA by using C programming language which provides a competitive security level with 1,024-bit RSA. The simulation consists of three components. Client side, Manager Side as well as cloud side.

MATHEMATICAL DEFINITION:

The goal of the algorithm is to divide the data DATA into n pieces (DATA1, DATA2, DATA3, DATA4 ….. DATA n) so that,

1. Retrieving any k or more DATA i pieces makes DATA easily computable.

2. Retrieving any k-1 or fewer DATA i pieces leaves DATA thoroughly undetermined.

The above scheme is known as threshold(k, n). if k=n, then all pieces are available for reconstruction of DATA.

The objective of Adi Shamir's secret sharing algorithm algorithm is that, k points are enough to define a polynomial of degree k-1.[1] Example, 2 points are sufficient to define a line.

Choose an approximate k-1 coefficients c 0 , c 1 , c 2 , c 3 ….c k-1 in H, and let c0 = S, where S is the Secret data which is going to be stored in cloud. Build the polynomial H(z) = c 0 + c1z 1 + c2 z2 +……+ck-1zk-1. Then n points are defined, for example set i=1,2….n to retrieve (i, H(i)) . A pair is formed with input to the polynomial and output. Given any subset of k of these pairs, using interpolation the coefficients of the polynomial can be found and the constant term is the secret.

SHAMIR'S APPROACH:

The secret is divided into pieces by considering an approximate degree polynomial

H(z) = c 0 + c1z 1 + c2 z2 +……+ck-1zk-1

In which c 0 = S, S1 = H(1), S2 = H(2),……., Sn = H(n)

EXAMPLE The following example illustrates the algorithm.

For understanding integer arithmetic is used instead of any other vector or scientific based arithmetic. Therefore the example provided does not ensure perfect secrecy, and is not a perfect example of Shamir's scheme.

ENCRYPTION AND PREPARATION

Consider 1999 as the secret data. Dividing it into 6 parts (n = 6). Parts required to reconstruct the secret is 3 parts (k = 3).

2 numbers are selected in random. Let it be 154 and 19. c1 = 154 and c2 = 19.

Our polynomial to produce shares are:

H(z) = 1999 + 154z + 19z2

6 parts are constructed from the polynomial.

(1, 2172) ; (2, 2383) ; (3, 2632) ; (4, 2919) ; (5, 3244) ; (6, 3607)

Different single point is given to each participant, both z and H(z).

RECONSTRUCTION

Any 3 points is enough to reconstruct the secret.

Assume: (a0, b0) : (2, 2383) ; (a1, b1): (4, 2919) ; (a2, b2) : (5, 3244)

Apply Lagrange basis polynomials:

l0 = a-a1/a0-a1 . a-a2/a0-a2 = 1/6a2 - 3/2a +10/3

l1 = a-a0/a1-a0 . a-a2/a1-a2 = 1/2a2 + 7/2a – 5

l2 = a-a0/a2-a0 . a-a1/a2-a1 = 1/3a2 – 2a +8/3

Therefore,

H(z) = 2383 (1/6z 2 - 3/2z +10/3) + 2919 (1/2z 2 + 7/2z – 5) + 3244 (1/3z 2 – 2z +8/3)

H(z) = 1999 + 154z + 19z 2

III.SOLUTION METHODOLOGY

Cloud customers may expect on behalf of their past experience and requirements. But the best approach is to gather information about the best and efficient cloud service provider. Customers are also prescribed to ensure the level of security of these important characteristics of the cloud: Confidentiality, Integrity and Availability (CIA). [4]

Security in Cloud computing is organized into different sections: security categories, security in service delivery models and security dimensions.

Security in cloud services is dependent on the following :

- Strong network security should be applied in and around the service delivery platform.
- Encrypting the data
- Access controls by authorization

Logs are to be strictly maintained and secured to note down the activities of the system administrators and other restricted users. They can also be used to produce reports that mix events relating to different customers of the service. Security should be applied and maintained in both the organizations seeking cloud solutions and the service providers. Identity and Access Management (IAM), Good governance, compliance, Availability, privacy, Data protection, Business Continuity and Disaster Recovery plans etc.. are some of the measures to ensure security in cloud.[5]

IV.CONCLUSION

we implement a secure data sharing system, Mona, for dynamic groups in an untrusted cloud. In Mona, a member is to share data with others in the group without revealing identity privacy to the cloud. Mona supports efficient user revocation and add new user. Efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files with encrypted format stored in the cloud before their participation. We implement One Administrator to handle Group manager and verify manager in revocation list Also we provide security by using OTP generation gives private key to each member. We proposed the satisfies the desired security requirements and guarantees efficiency as well.

V.REFERENCES

[1] Kanya Devi J, Kanimozhi S Assistant Professor Department of Computer Science and Engineering Sri Shakthi Institute of Engineering and Technology Coimbatore-62

[2] W.H Sun, W.J Lou, Y.T Hou, and H Li, "Privacy-preserving keyword search over encrypted data in cloud computing," in Secure Cloud Computing. Springer, 2014, pp. 189–212.

[3] 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. 2015

[4] Md Kausar Alam, Sharmila Banu K, "An Approach Secret Sharing Algorithm in Cloud Computing Security over Single to Multi Clouds", International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013

[5] 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.