ISSN 2348 – 7968

Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud

Rohit Pingale
Computer Department, Pune University, Pune, Maharashtra, India,
Rahul Hume
Computer Department, Pune University, Pune, Maharashtra, India,
Tushar Pawar
Computer Department, Pune University, Pune, Maharashtra, India,
Nikhil Rasal
Computer Department, Pune University, Pune, Maharashtra, India

Abstract :

In this paper, 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.

Keywords Cloud Computing, Data Sharing, Group Signature, Dynamic Groups, User Revocation, Access Control

1.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 datacenters. 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.

2. LITERATURE SURVEY:

Sr no	Title of paper	Author	Year of publication	Problem describe with solution	Future Work
1	Mona:Multi owner data sharing	Guangtao Xue,Zhongwei Li &Yunhuai Lu	IEEE2009	Static models for route prediction. Centralized approach	To make this approach distributed
2	On prediction using variable order markov model	Ron Beglieter, Ran EL-yaniv	Journal of artificial Intelligence Research 2004	Description of different algorithm for prediction	Implementation of new algorithm
3	Route prediction from Trip observation	Jon Froehlich and John Krumm	2008 SAE International	route prediction for long term routes	Prediction using geographic distance algorithm
4	A Markov Model for driver turn	John Krumm	2008 SAE International	Algorithm for short term route for	Implement algorithm for long term route

	prediction			vehicle drivers	prediction
5	Learnig to predict driver route and destination	Ried semmeous, BretBrownning	General Motors	Route prediction using HMM	To make this appraoch suitable for real

Table 1: Literature Survey

3. EXISTING SYSTEM:

In existing system the security schemes study about several method for secure data sharing on untrusted cloud. The only data owner or group manager has the authority to share and stored the files on untrusted cloud. Thus the data owner or group manager can send private decryption keys to the authorised users. Thus the out side users or storage server can't read the contents of the file as they are unaware of private encryption keys. Thus the complexity of the new users is increasing with no of data users and the no of revoked users respectively..Old system develop new crypto system for fine-grained sharing data and the no of revoked users based on key-policy attribute based encryption (KP-ABE).

The solution for preserving data privacy is to encrypt the data and then it can be stored on the cloud. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task. Thus in the existing system the only data owner or group manager has the authority to share and stored the files on untrusted cloud. Thus the data owner or group manager can send private decryption keys to the authorised users. Thus the out side users or storage server can't read the contents of the file as they are unaware of private encryption keys.

MONA MODEL:

In the security schemes we have study about several method for secure data sharing on untrusted cloud. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task. To overcome the problem occured by the existing system, the new method is implemented called as MONA. The MONA presents the new method for secure data sharing and storing on untrusted cloud. In this, user is able to share data with others on cloud without reveling the identity privacy. In addition to this, it allows new user joining and users revocation list. The new users can decrypt files stored on the cloud without participating. The user revocation can be found out by using public revocation list without updating private keys of another users.

The MONA[1] consist of three main different entities

1)Group manager

2)Group member

3)Cloud server

Disadvantages:

Only the group manager can store and modify data in the cloud. The changes of membership make secure data sharing extremely difficult the issue of user revocation is not addressed.

4. SYSTEM MODEL AND ITS DESIGN GOALS

4.1 SYSTEM MODEL:

We design a cloud computing architecture by combining with an example of organization uses to its staff in same group or department to store and share data. The system model has four parts such as System Admin, group manager, large number of group members and cloud.

Cloud is like a server to store the data and maintain the data securely. Cloud is operated on CSP i.e. Cloud Service Provider by them storage as service and provides large storage services. Cloud is not fully trusted on users. We assume that the cloud server is honest and trust them. So Cloud server will not maliciously delete or modify user data due to security of data, but users try to learn data by using own identities of cloud.

Cloud Computing
Cloud computing the word cloud is used as a “the Internet” so the phrase cloud computing means "a type of Internet-based computing," where different services -- such as servers, storage and applications -- are provide to an organization's computers and devices through the Internet in lower cost.

System Administrator is controls the group manager and add the group managers and assign to each department uniquely, deactivate the managers to revocation list, maintain the log details of managers. System Admin is control overall groups.
System Administrator Module
System Admin takes charge of followings,
1. System initialization,
2. Manager registration,
3. Manager revocation

Group manager controls the system generation, user registration, user revocation, and
revealing the real identity of a dispute data owner. In the given example manager is the group manager of each department wise. Therefore, we assume that the group manager is fully trusted by the other parties.
Group Manager Module
Group manager takes charge of followings,
1. System parameters generation,
2. User registration,
3. User revocation, and
4. Revealing the real identity of a dispute data owner.
Therefore, we assume that the group manager is fully trusted by the other parties.
The group manager is take the responsibility of user registration and also user revocation.
Group members are the registered users they will upload their private data into the cloud server and share the data among the group members. In our example, the employee plays the role of group members. It allows the group members changed, due to the staff resignation and the participation of new employee in the organization.
Group Member Module
Group members are registered users that will
1. Store their private data into the cloud server and
2. Share them with others in the group.
The group member are the owners of changing the files in the group and they are modify it.
File Security Module
1. Encrypting the data file.
2. 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)

Group Signature Module

A group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. The designated group manager can reveal the identity of the signature's originator when a dispute occurs, which is denoted as traceability.

User Revocation Module

User revocation is performed by the group manager by revocation list (RL), based on which group members can encrypt their data files and ensure the confidentiality against the revoked users.

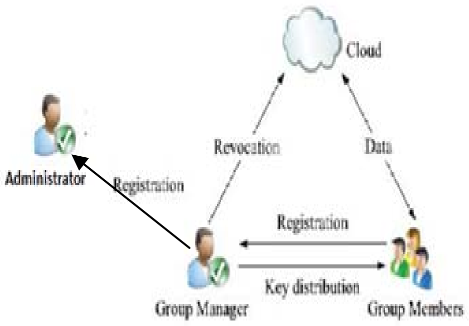

Fig. 1 System Model.

4.2 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, authorizes 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 removed into the cloud after the revocation. Data owner will store the data on 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.

5.THE PROPOSED SCHEME: MONA

5.1 Overview

MONA is multi owner data sharing to achieve secure data sharing for dynamic groups in the cloud. we used to combine the group signature and dynamic broadcast encryption techniques. Specially, the group signature scheme enables users to anonymously use the cloud resources and the dynamic broadcast encryption technique allows data owners to securely share their data files with others group members including new joining users.

But each user has to compute revocation parameters to protect the confidentiality from the revoked users in the dynamic broadcast encryption scheme.

To overcome 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 cipher text size. Specially, the computation overhead of users for encryption operations and the cipher text size is constant and independent of the revocation users.

This MONA system provide efficiency, scalability and most importantly reliability.

In MONA group member access and upload the data by using encryption algorithm(AES) and use private key.

5.2Advantages:

1.To overcome the disadvantage of existing system MONA, in the proposed MONA system is

generate the OTP(one time password) due to that group member receives the private by mail and access the data or to share the data on cloud and provide the more security.

2.Also group member upload the data in encrypted format due to that unauthorized user or attacker will not access the data.

3.Another advantage is we declare the System Administrator to handle the overall system control or to handle the all group managers and maintain the log of managers.

4.Also we provide the revocation list to remove the unauthorized users and they unable to access the data over the cloud.

Scheme Description

This system describe system initialization, user registration, user revocation, file generation, file deletion, file access and traceability.

System Initialization

The System Administrator takes charge of system initialization generating a bilinear map group system. First Admin allocate the group managers to each group or department.

Maintain the log detail of managers.

User Registration

The group manager takes the charge of user registration. When any new user assign any particular group or add the new user then manager register the new user. And maintain the log details of group members.

After the user registration user obtain the private key and used group signature for file generation and file decryption.

User Revocation

User revocation is performed by Administrator to remove the group manager. And performed by Group maanger to remove group members based on encrypt data files and ensure the confidentiality against revoke users. Admin and group manager update the revocation list each day.

File Generation

To store and share the data on the cloud a group member is perform operations.

Group ID	Data ID	time	ciphertext	hash	signature
IDgrouop1	IDdata1	T1	C1	F(µ1)	S1
IDgroup2	IDdata2	T2	C2	F(µ2)	S2
IDgroup3	IDdata3	T3	C3	F(µ3)	S3

When member share or access the data first send the group identity or ID of member then the cloud verify the revocation list is this authorized user or not. Otherwise failed to generate the file.

Second is verifying the signature. If this all are valid then member can generate the file and share it on group.

Table 1: Message format for uploading data

File Deletion

File store on cloud is delete by either group manager or data owner (who upload the data). To delete the file ID data and group signature is required and send it to cloud. Then cloud will delete the file.

File Access

File access means to load the data on cloud by group members. But this process is similar to file generation. First verify the valid user using revocation list and group ID data. If user is valid then give access to data otherwise failed to access.

Traceability

When data dispute occurs then tracing is used to performed by group manager to identify the real data owner

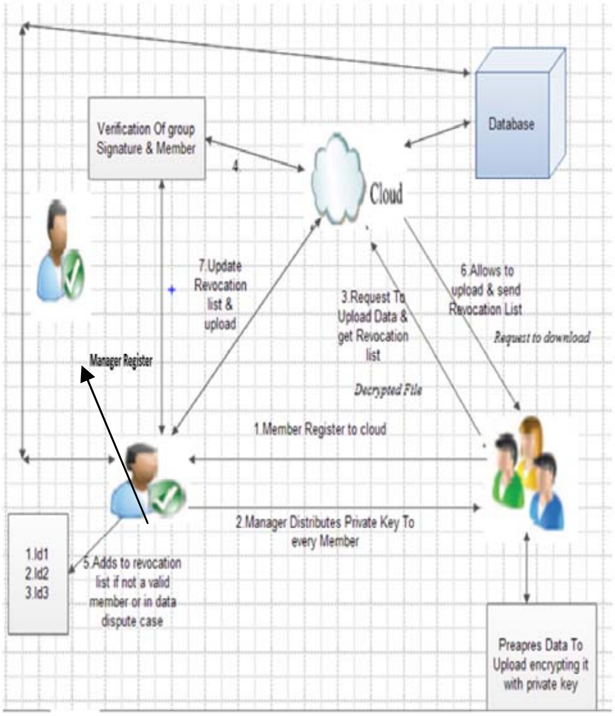
Database
Verification Of group Signature & Member
4
Cloud
7.Update Revocation list & upload
3.Request To Upload Data & get Revocation list
6.Allows to upload & send Revocation List
Request to download
Manager Register
Decrypted File
1.Member Register to cloud
2.Manager Distributes Private Key To every Member
1.Id1
2.Id2
3.Id3
5.Adds to revocation list if not a valid member or in data dispute case
Preapres Data To Upload encrypting it with private key

Fig. 2 Proposed Scheme MONA.

6.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.

7.References:

[1] D. Boneh, X. Boyen, and H. Shacham, "Short Group
Signature," Proc. Int'l Cryptology Conf. Advances in
Cryptology (CRYPTO),pp. 41-55, 2004.

[2] D. Boneh and M. Franklin, "Identity-Based Encryption
from the Weil Pairing," Proc. Int'l Cryptology Conf.
Advances in Cryptology (CRYPTO), pp. 213-229, 2001.

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

[4] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of
Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

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

[6] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing,"
Proc. IEEE INFOCOM, pp. 534-542, 2010.

[7] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM
Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[8] 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.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf.
Computer and Comm. Security (CCS), 2006.

[10] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in
Cryptology (CRYPTO), pp. 41-62, 2001.