IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

Secure Multi-Owner Data Sharing for Dynamic Groups in Cloud

Ms. Nilophar M. Masuldar[1], Prof. V. P. Kshirsagar [2]

Research Scholar, Computer Engineering Department, Government Engineering College, Aurangabad, India[1]

Head of Department, Computer Engineering Department, Government Engineering College, Aurangabad, India[2]

Abstract: Cloud computing provides the efficient use of resources over the internet. In this paper a secure multi owner data sharing scheme for dynamic groups in cloud is proposed. By generating the group signature and encryption technique the user can anonymously store and share the data. When the new user registration is done a group signature is given to the user belonging to a particular group. While downloading the data from the cloud the user has to enter the group signature and secret key which will be received to the user via an e-mail. When both the entities will match then only the user is able to download the data.

Keywords: Multi owner, dynamic broadcast encryption, group signature, user revocation

I. INTRODUCTION

Cloud computing provides the data sharing and storing it among the users with the less cost and efficient use of resources over the internet. Cloud computing provides the resources and software to the users as per their need. Cloud computing makes the provision for the users to store their data remotely on the cloud and make it available for the users belonging to the same group, their by generating the group signature. Cloud data centers are facilitating the users by providing various services. let us consider an example ,in a company there are various staff members working on different modules and they are on different locations. if the data is to be stored and shared then there is problem of security arises because the cloud service providers are not trustworthy for this reason the data needs the encryption methods before it is stored on the cloud. In these models, the data owners store the encrypted data on untrusted cloud. Most of the secured techniques have been suggested for securely storing the data. The members will exchange the decryption keys and they can decrypt the data. This prevent the cloud service providers and attackers to access the encrypted file, as they don't have the decryption keys. However the new data owner registration in the above said models reveals the identity of the new data owner to the other in the group. The new data owner has to take permission from other data owners in the group before generating a decryption key. The proposed system identified the problems during multi owner data sharing and proposed an efficient way using group signature and cryptographic techniques for solving limitations in the traditional approach. In this paper a secure multi owner data sharing scheme is implemented in which the group signature is generated during the registration of new user and while downloading the files from the cloud, secret key will be sent to the e-mail id of the user. Hence, the data can be downloaded without contacting with the data owner just by providing the group signature and secret key.

II. LITERATURE REVIEW

Cloud computing is used for many developing education area and organizations. The most important role of cloud comes because of its ability to provide the services, platform and infrastructure as resources. It includes software storage, security data which will be allocated to the users as per the demand.

1. Scalable Secure File Sharing on Untrusted Storage.
A cryptographic system Plautus enables secure file sharing without having to trust on the file servers. It efficiently uses cryptographic techniques to protect and share the files. Plautus features are highly scalable key management while allowing individual users to maintain control over accessing of the files.

2. Securing Remote Untrusted Storage
In this paper Sirius, a secure file system designed for insecure network and p2p file system. sirius assumes that the network storage is untrusted and provides its own read write cryptographic access control for file level sharing.

A.EXISTING MODEL: 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

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

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 outside users or storage server can't read the contents of the file as they are unaware of private encryption keys. In the security schemes we have study about several methods 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 occurred 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 revelling 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 other users.

The system consist of three main different entities

1) Group manager
2) Group member
3) Cloud server

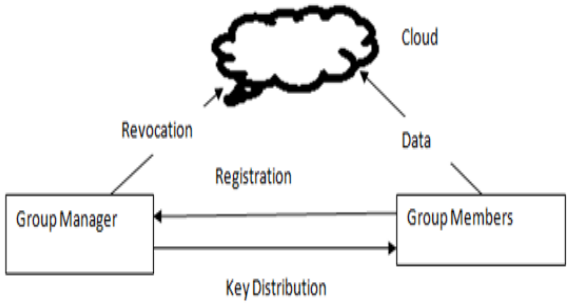


Fig.1 Existing System

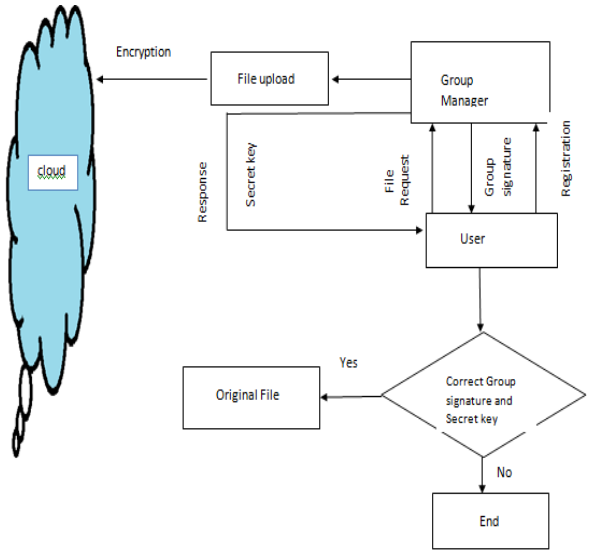
Limitations

1.Revocation of user leads to change of private keys of all the group members.

2.Any user in group is able to encrypt the files and other users are able to decrypt.

B. PROPOSED MODEL AND ITS DESIGN GOALS

In this paper, Mona protocol for secure data sharing in the cloud computing is proposed. This scheme supports dynamic groups efficiently. A secure and privacy preserving access control to the users is provided in this scheme which enables the users to anonymously utilize the cloud resource. The newly registered user can directly decrypt the files without contacting with the data owner. The identities of the data owners are kept confidential and whenever it is needed to reveal their identities the group manager when dispute occurs. The user revocation can be done easily without disturbing the secret keys of the existing users.



g: Proposed System Architecture

Advantages of proposed system

1. New user in the group can use the files by decrypting it without contacting with data owners.
2. User revocation can be easily done without updating the secret keys of the remaining users.
3. Secret key is sent via an email for more security.

In this scheme, various modules are used as

1. Group Manager Registration
2. Group signature generation
3. Group Member Registration
4. Revocation

The manager takes charge of the following

The group manager registration module is used for registration of the manager and a manager will be given an id and a password. The manager can upload the files into the cloud by encrypting it with the public key. A pair of public and secret keys will be generated for uploading.

Algorithm used

1. Group signature generation: The manager will generate the group signature that will be given to the user while registration process.

2. Group Member Registration: The new user will register to the group and a group signature will be given to the user. When the member is registered with a particular group then he can access the files by sending the request to the manager for that file. On getting the request from the user the manager will send the secret key to the user in response via an e-mail. The user can download the requested file by using the secret key and the group signature.

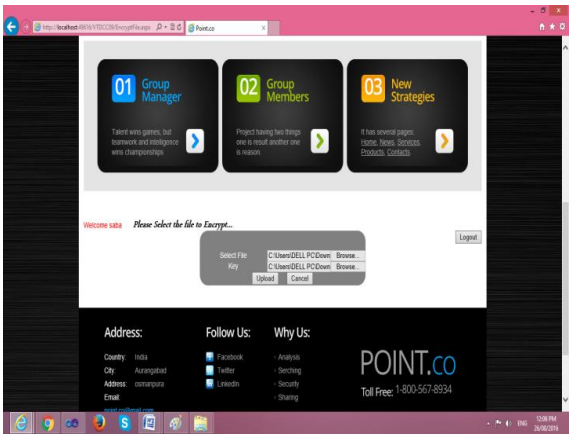
3. Revocation: user revocation can be done if the member resigns, then the manager will revoke the user by maintaining the revocation list without updating the secret keys of the remaining users.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

Experimental Method

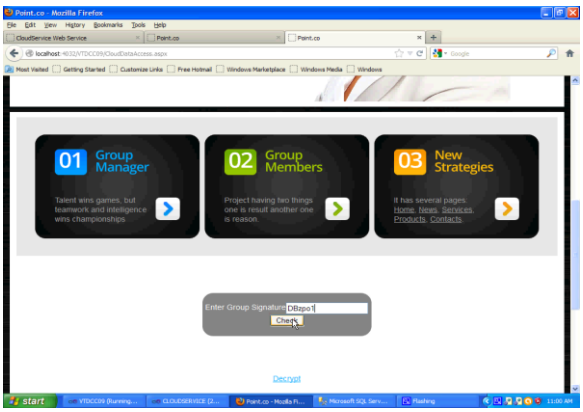
Parameters	Existing System	Proposed System
Operation	Single owner	Multiowner
Security	Low	More(Group signature is used)
Algorithms	DES	RSA
Performance	Low	High
Group	Static	Dynamic
Revocation	Changes the keys of existing users	Did not change the keys of existing users.
Encryption Technique	Public Key Cryptography	Broadcast Encryption
Revocation Mechanism	Inefficient	Efficient
Key Distribution	Dependant on revoked users	Independent of revoked users

File Uploading



Group manager encrypts the files by public key and upload the files on the cloud server.

Group Signature verification

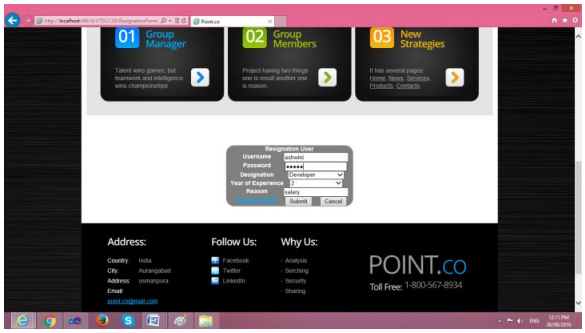


On successful user registration user will be given the group signature by the manager to the user, while downloading the files from the cloud the user has to enter the valid group signature. if the group signature is valid then only the user can get the files from the cloud.

Revocation

When the resigns, the request will be sent to the manger and if the manager approves it then the user will be revoked successfully. Once the user is revoked from the system then he will not be able to access the files on the cloud. In this case the existing user's private keys will not be changed.

Revocation



III. CONCLUSION

The suggested scheme provides the secure data sharing and storing the data on cloud more efficiently. The manager can upload the files; the use of group signature and encryption techniques makes the system more secure. Sending secret keys to the users via an e-mail gives more security to the data. User revocation is done without updating the secret keys of the remaining users.

REFERENCES

[1] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 6, JUNE 2013

[2] Scalable Secure File Sharing on Untrusted Storage by Mahesh Kallahalla,Erik Riedel ,Ram Swaminathan,Qian Wang,Kevin FU.

[3] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.

[4] Ms. Shrayu P. Pachgade, Asso. Prof. K. G. Bagde A Secure Data Sharing Application for Dynamic Groups in the Cloud, Volume 4, Issue 10, October 2014

[5] G.Bhanu Prasad, C.Harsha Vardhini 'Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud' ISSN (Online): 2347-2820, Volume -3, Issue-11 2015

[6] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.