Volume: 07 Issue: 05 Pages: 2899-2903 (2016) ISSN: 0975-0290

Multi Owner Data Sharing & Outsourced Revocation Using Identity Based Encryption on Cloud

K.Kowsalya[1]
Department of Computer Science & Engineering
Kalasalingam Institute of Technology
Krishnan Koil, India
Email: Kowsalya30992@gmail.com
V. Ramesh[2]
Assistant Professor, Department of Computer Science & Engineering
Kalasalingam Institute of Technology
Krishnan Koil, India
Email: prof.rameshv@gmail.com

ABSTRACT

Cloud computing is an economical and effective solution for sharing group resource among cloud users. Unfortunately, sharing data in a multi-owner manner while protect data and identity privacy from an un trusted cloud is still a challenging issue, due to the recurrent change of the membership.The major aims of this method a secure multi-owner data sharing scheme.That is any user in the group can securely share data with others by un trusted cloud. Moreover, the real identities of data owners can be exposed by the group manager when disputes occur. User revocation can be achieved by a novel revocation list and no need to update the secret Keys of the remaining users.The drawback of IBE is computation over head. To overcome the drawback introduces outsourcing computation.

Keywords: **Cloud Computing; Revocation; Multi owner data sharing; Identity based encryption**

Date of submission: March 24, 2016 Date of Acceptance: April 28, 2016

1. INTRODUCTION

Cloud Computing is a general term used to describe a new class of network based computing that takes place over the Internet and it is encapsulating the delivery of computing resources as a service.It is an efficient solution for sharing group resources among cloud users. The goal of cloud computing is to apply traditional Supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.Identity based encryption is a public-key encryption in which the public key of a user is some unique information about the identity of the user (e.g. a user's email address).secure multi-owner data sharing scheme is implies that any user in the group can securely share data with others in the untrusted cloud. identity privacy is one of the most significant obstacles for the wide deployment of cloud computing. Without the guarantee of identity privacy, users may be unwilling to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers. On the other hand, unconditional identity privacy may incur the abuse of privacy.

2. RELATED WORKS

E. Goh, H. Shacham, N. Modadugu, and D. Boneh [5] 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. Extensions to SiRiUS include large scale group sharing using the NNL key revocation construction.

V. Goyal, O. Pandey, A. Sahai, and B. Waters [7] they develop a new cryptosystem for One-grained sharing of encrypted data that call Key-Policy Attribute-BasedEncryption (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-

Volume: 07 Issue: 05 Pages: 2899-2903 (2016) ISSN: 0975-0290

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.

S. Kamara and K. Lauter [8] 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 our 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 [4] 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

3. THEORETICAL ANALYSIS

3.1 PROJECT SCOPE

The scope of the project is to provide multi owner data sharing and revocation method. Multi owner data sharing scheme is mainly used for sharing purpose and revocation is mainly used to provide security purpose.

3.2 PROBLEM STATEMENT

In existing system only single owner group is present.The single owner manner hinders the adoption of their scheme into the case where any user is granted to store and share data.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. Security is very bad. User revocation is very difficult.

3.3 PROPOSED SYSTEM

The goal of this project is to provide multi owner data sharing scheme and provide high level security.

3.3.1 Multi Owner Data Sharing Scheme

A secure multi-owner data sharing scheme is implies that any user in the group can securely share data with others by the untrusted cloud. Our proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users. A secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource, is provided. Moreover, the real identities of data owners can be revealed by the group manager when disputes occur. A rigorous security analysis, and perform extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead.

3.3.2 AES algorithm

AES algorithm is used for security purpose.The following steps are done.
Step 1:Derive the set of round keys from the cipher key.

Step 2:Initialize the state array with the block data (plaintext).

Step 3:Add the initial round key to the starting state array.

Step 4:Perform nine rounds of state manipulation.

Step 5:Perform the tenth and final round of state manipulation.

Step 6:Copy the final state array out as the encrypted data (ciphertext).

The process of executing a program or application with the intent of finding software bugs.

Volume: 07 Issue: 05 Pages: 2899-2903 (2016) ISSN: 0975-0290

4. SIMULATION SYSTEM DESIGN

4.1 Architectural Diagram

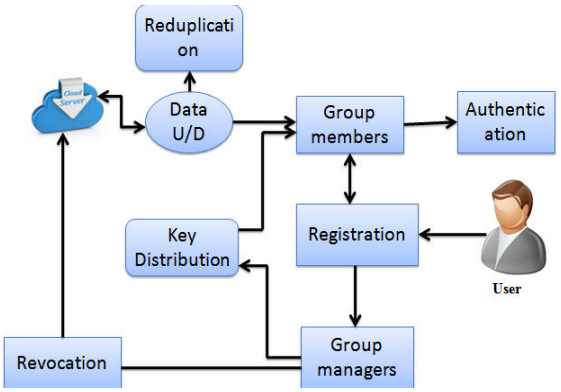

Fig 4.1:Architectural Diagram

Architecture design representation multi owner data sharing scheme.First user have to register their details.All group members are under the control of group manager and all group manager are under the control of administrator. Group member can have to upload and download the files from cloud server.If any user in the group should be malicious than revocate that user from the group.Group manager distribute the key to the group members for download purpose.Group members can be authendicated by google app engine.

5. RESULTS

It Provide multi owner date sharing scheme and revocation techniques. It overcome the problem of single owner data sharing and provide high level security

5.1 Screen shots

Software testing is an investigation conducted to provide stakeholders with information about the quality of theproduct or service under test. Software testing also provides an objective, independent view of the software to allow the business to appreciate and understand the risks of software implementation. Test techniques include, but are not limited to, the .

5.1.1 User Registration

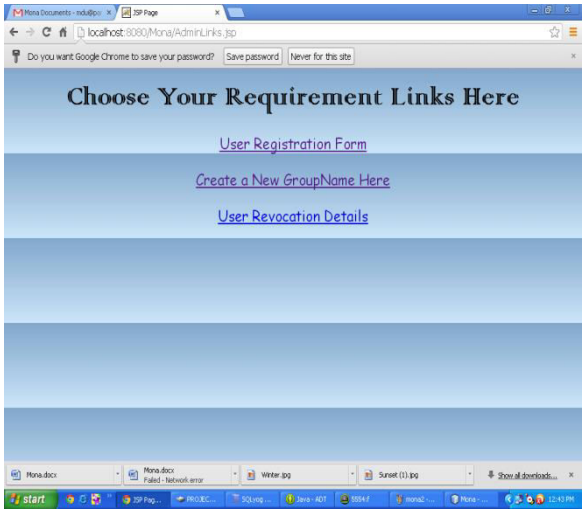

Fig 5.1.1.User Requirement Selection

The first process is to any one from the list.If new user came then the user has to do registration process.If they want to new group then select Create a New GroupName Here option.To view the Revocation details from the User Revocation Details option

5.1.2 New User Registration

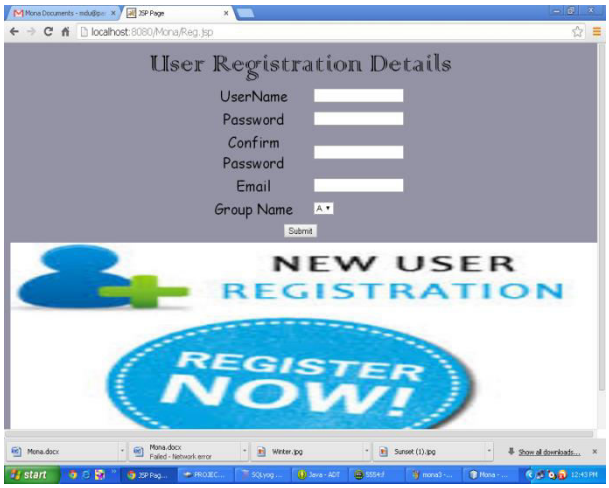

Fig 5.1.2 User Registration

Here the user have to register their details for their registration process. Give their user name, password, email-id and select the group name which group belongs to.

Volume: 07 Issue: 05 Pages: 2899-2903 (2016) ISSN: 0975-0290

5.1.3 Group Name Registration

Fig 5.1.3 Group Name Registration

Here the group manager create the Group Name and Group Key for the newely created group.

5.1.4 File Upload

Fig 5.1.4 File Upload

Here the user want to upload the file, choose the file which are going to be upload,from the particular place and then click the submit option. Then the file will be upload successfully.

5.1.5 File Deletion

Fig 5.1.5 File Deletion

Here the user want to delete the file, select the file which are going to be delete and then click the delete option.

5.1.6 User Signout

Fig 5.1.6 User Signout

Atlast the user have to Sign Out from the Group or to give request to other file group or to download other group file.

6. CONCLUSION

To design a secure data sharing scheme for dynamic groups in an untrusted cloud. In this a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, it 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. Extensive analyses show that our proposed scheme satisfies the

Volume: 07 Issue: 05 Pages: 2899-2903 (2016) ISSN: 0975-0290

desired security requirements and guarantees efficiency as well.

FUTURE WORK

The enhancement of this project will be how to avoid some type of re-computation introduced by dynamic groups while still preserving identity privacy from the public verifier during the process of public data on shared data.

REFERENCES

[1] Alexandra Boldyreva, Vipul Goyal, and Virendra Kumar" Identity-based Encryption with Efficient Revocation" CCS 2008, ACM Press, 2008.

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

[3] Craig Gentry "Certificate-Based Encryption and the Certificate Revocation Problem" DoCoMo USA Labs.

[4] Fiat A and Naor M, "Broadcast Encryption," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.

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

[6] 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.

[7] Goyal V.Pandey O, Sahai A, and Waters B, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data, "Proc. ACM Conf. Computer and Comm. Security (CCS), pp.89-98, 2006.

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