International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

A Secure Anti-Conspiracy Information Sharing Scheme for Dynamic Groups in the Cloud Server

Megha L[1], Bhagyashri R Hanji[2], Dr. Kavitha K S[3], Dr. Kavitha C[4]

[1]PG Student, Department of CSE, Global Academy of Technology, Bengaluru, Karnataka, India
[2]Assistant Professor, Department of CSE, Global Academy of Technology, Bengaluru, Karnataka, India
[3]Professor, Department of CSE, Global Academy of Technology, Bengaluru, Karnataka, India
[4]Professor & HOD, Department of CSE, Global Academy of Technology, Bengaluru, Karnataka, India

---

Abstract – *Cloud Computing provides the user an effective way for the sharing data among the group members in the cloud with reasonable maintenance and minimal management cost. In order to provide the security for the sharing data is very challenging task as the data files are outsourced. As to achieve the privacy of the data is still an issues because the members in the group are changing and mainly the users those do not exist in the current group may share the data files from the untrusted cloud. In order to achieve the security and privacy preserving of the data is more difficult in the existing schemes as the key are obtained through the secure communication channel. In this paper, a secure information sharing scheme for the dynamic groups is proposed where the users obtain their private keys directly from the group manager securely as the key distribution is done without any secure communication channel. The scheme can achieve greater efficiency as the existing users need not to update their private keys even if the users are revoked from the group or when a new user is added to the group. A secure user revocation is achieved in which the scheme is protected from the Conspiracy attack.*

Key Words: **Cloud Computing, privacy preserving, Key Distribution, security, Conspiracy attack.**

1.INTRODUCTION

Cloud Computing is a model for enabling on demand access to the shared pool of the configurable computing resources which can be rapidly provisioned with a minimal management effort. Cloud Computing and storage solutions provide users with various capabilities to store and process their data in the cloud[1]. Cloud Computing relies on sharing of the resources to achieve scalability. Here a secure information sharing scheme for the dynamic groups is proposed. This paper, mainly presents the following scheme: The users obtain their private keys directly from the group manager securely as the key distribution is done without any secure communication channel. Greater efficiency is achieved where the existing users need not to update their private keys even if the users are revoked or when a new user is added to the group. The scheme is protected from conspiracy attack.

2. EXISTING SYSTEM

Here in the existing techniques of Cryptographic storage system the data sharing was not secure because of the untrustworthy servers where the data files are divided into file groups and the each file group is encrypted with a file-block key[2].Where the file-key needs to be updated so the system had a heavy Key distribution overhead. In the existing scheme the data sharing is on the untrusted servers so due to the increase in the number of revoked users and data owner, there is complexity in the revocation and user involvement[3]. A key policy attribute-based, proxy re-encryption and lazy re-encryption techniques were used in the existing system where without disclosing the content scheme achieved the fine-grained data access control. Due to this any users in the group can share and store the data with others by using the cloud service[4].

3. PROPOSED SYSTEM

In this paper, a secure data sharing scheme is proposed where user can achieve secure key distribution and information sharing for dynamic group. A secure information sharing scheme for the dynamic groups is proposed where the users obtain their private keys directly from the group manager securely as the key distribution is done without any secure communication channel. The scheme achieves fine-grained access control where any users in the group can access the cloud and the users which are revoked cannot access the cloud again after they are revoked. A secure user revocation is achieved in which the scheme is protected from the Conspiracy attack where the revoked users will not be able to obtain the original data once after the revocation. The scheme can achieve greater efficiency as the existing users need not

to update their private keys even if the users are revoked from the group or when a new user is added to the group. The architecture has three entities such as cloud, Group Manager, and Group Members. Cloud Server provides the storage space for uploading the data files. Group Manager does the generation, user registration and user revocation. Group Members are set of registered users store their own data into the cloud.

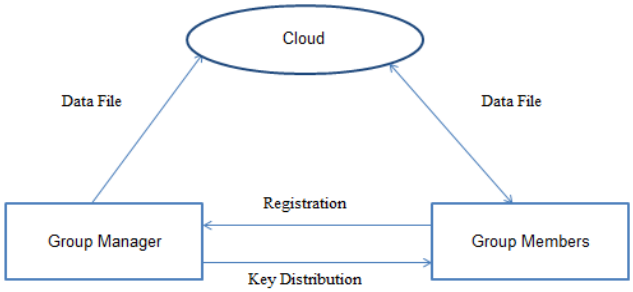

Fig -1: Proposed System Architecture

The architecture is split into following modules as shown in Fig-1:

3.1 User registration and login:

In the user registration module, new user will register to the particular group with a user name and password, then the user can upload the file to the cloud and download file from the cloud.

3.2 File Uploading Process:

In the file uploading process module, user will select the particular file that needs to be uploaded and after providing the credentials, the selected file will be uploaded to the cloud successfully.

3.3 File Downloading Process

In the file Downloading process module, user will select the filename that needs to be downloaded from the cloud from the particular group. As soon as the downloading process is completed the user can view the files which the user had downloaded.

4. PERFORMANCE EVALUATION

Performance evaluation of the proposed work is shown in the following figure.

The uploading of the file to the cloud is shown in the Fig-2: which has the file uploading time of the file and the file size.

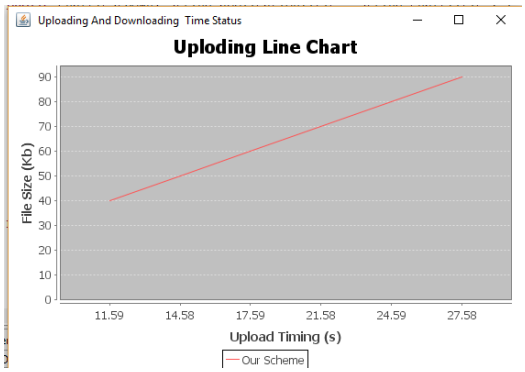

Fig -2: Uploading the file

The downloading of the file from the cloud is shown in the Fig-3: which has the file downloading time of the file and the file size.

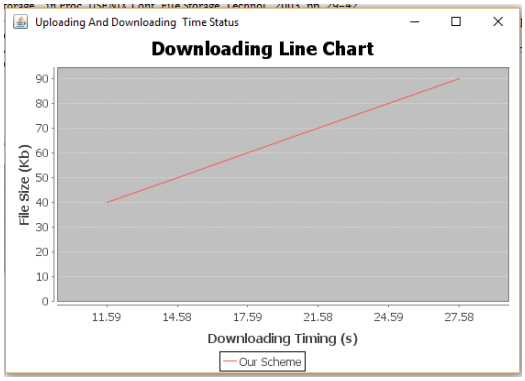

Fig -3: Downloading the file

5. CONCLUSIONS AND FUTURE WORK

The proposed scheme achieves the secure anti-conspiracy information sharing scheme for the dynamic users in the cloud where the users securely obtain their private keys from the group manager without any communication channel. The scheme is protected from the conspiracy attack and also the scheme has greater efficiency as the existing users need not to update their private keys even if the users are revoked from the group or when a new user is added to the group.

In the proposed work , a secure data sharing is done where the data owner can share data with the members of his group and it prevents outsiders from gaining any data access in case of malicious activities such as data loss and theft. However, there is always a chance that the group members can share the data by

making the illegal copies and distributing to friends, general public, etc for profit. In the future, the data owner can create a set of access control rules on his data and send the data along with the access control policy. If a member attempts to make illegal copies of the data, the access control policy should "lock" the data to prevent the member from doing so. Also, since data stored in the Cloud are usually stored and replicated in different geographical locations around the world, it is important that the legitimate rules are followed. So it would be to find ways to store and process data in a way that does not breach the privacy and security laws of the region.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, Apr. 2010.

[2] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proc. USENIX Conf. File Storage Technol., 2003, pp. 29–42.

[3] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. Netw. Distrib. Syst. Security Symp., 2005, pp. 29–43.

[4] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282–292.

[5] S. Kamara and K. Lauter, "Cryptographic cloud storage,"inProc.Int.Conf.FinancialCryptographyDataSecurity,Jan.2010,pp.136–149.