International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 04 | April - 2022 Impact Factor: 7.185 ISSN: 2582-3930

A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud

Chirunth R[1] and Murugan R[2]

[1]Research Scholar, School of Computer Science and Information Technology, JAIN (Deemed to be University), Bangalore, India

[2]Associate Professor, School of Computer Science and Information Technology, JAIN (Deemed to be University), Bangalore, India

ABSTRACT

A secure data-sharing scheme for dynamic members. Firstly, we propose a secure way for key distribution without any secure communication channels, and the users can securely obtain their private keys from group manager. Secondly, our scheme can achieve fine-grained access control, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked. Thirdly, we can protect the scheme from collusion attack, which means that revoked users cannot get the original data file even if they conspire with the untrusted cloud. In our approach, by leveraging polynomial function, we can achieve a secure user revocation scheme. Finally, our scheme can achieve fine efficiency, which means previous users need not to update their private keys for the situation a new user joins in the group or a user is revoked from the group.

1. INTRODUCTION

Data sharing has become an increasingly important topic in the business world. Traditionally defined as a concept in the world of academic research, data sharing as a technology has become highly relevant for businesses of all sizes, whether they need to disseminate data across a large, global organization or need to augment internal data with broader market data to gain better insights. The sharing of data securely in cloud computing is a very crucial method. The information is stored in cloud data centers. To access data from or store data into data centers through the internet, the intruders may attack our data. Users can achieve an effective and economical approach for data sharing among group members in the cloud with the characters of low maintenance and little management cost. Meanwhile, we must provide security guarantees for the sharing data files since they are outsourced. Unfortunately, because of the frequent change of the membership, sharing data while providing privacy-preserving is still a challenging issue, especially for an untrusted cloud due to the collusion attack. Moreover, for existing schemes, the security of key distribution is based on the secure communication channel, however, to have such channel is a strong assumption and is difficult for practice.

2. RELATED WORKS

"A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud ". It provides a secure way for key distribution without any secure communication channels. The users can securely obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user. The problem is to propose professional public-key encryption pattern that supports stretchy allocation in the logic that every subset of cipher data is decrypt by invariable size decryption key. The most abundant problem is to successfully distribute encrypted data. The

algorithms used in this paper are AES Algorithm, Ring Signature. In this paper, to design a protected anti-collusion facts sharing scheme for dynamic companies in the cloud. As the group member receives hierarchical key that only one person can access the data, which is most useful step in this paper, so as multiple request arrives it is easy to handle the clients with help of group key manger technique.[3]

3. PROBLEM FORMULATION

Kallahalla et al presented a cryptographic storage system that enables secure data sharing on untrustworthy servers based on the techniques that dividing files into file groups and encrypting each file group with a file-block key. Yu et al exploited and combined techniques of key policy attribute-based encryption, proxy re-encryption and lazy re-encryption to achieve fine-grained data access control without disclosing data contents. The file-block keys need to be updated and distributed for a user revocation; therefore, the system had a heavy key distribution overhead. The complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the revoked users. The single-owner manner may hinder the implementation of applications, where any member in the group can use the cloud service to store and share data files with others.

4. SYSTEM ANALYSIS

Data Sharing in Cloud modern cloud data sharing is changing the scope of what is possible for data sharing. With cloud data sharing. Organizations can enable the following:

- Data sharing for business efficiencies: Share live data with internal and external business partners to optimize spend, provide superior customer service, and streamline operations.
- Data sharing to eliminate data silos: Create a single source of truth for all internal data and share it with thousands of internal data consumers across hundreds of business units within a single organization.
- Data sharing as a product (data provider): Provide direct access to specific data sets as a monetized service for data consumers to augment their existing data.
- Data sharing as a product differentiator: SaaS providers can offer direct access to the petabytes of data generated from their B2B customer activity. To fully leverage data sharing in the cloud, businesses will require a platform with speed, power, governance, security, and ease of use.
- Simple Mail Transfer Protocol (SMTP) is used to send and receive email. It is sometimes paired with IMAP or POP3 (for example, by a user-level application), which handles the retrieval of messages, while SMTP primarily sends messages to a server for forwarding.

5. PROPOSED SYSTEM

Design Phase: We describe the main design goals of the proposed scheme including key distribution, data confidentiality, access control and efficiency as follows:

1. Key Distribution: The requirement of key distribution is that users can securely obtain their private keys from the group manager without any Certificate Authorities. In other existing schemes, this goal is achieved by assuming that the communication channel is secure, however, in our scheme, we can achieve it without this strong assumption.
2. Access control: First, group members are able to use the cloud resource for data storage and data sharing. Second, unauthorized users cannot access the cloud resource at any time, and revoked users will be incapable of using the cloud resource again once they are revoked.
3. Data confidentiality: Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of the stored data. To maintain the availability of data confidentiality for dynamic groups is still an important and challenging issue. Specifically, revoked users are unable to decrypt the stored data file after the revocation.

4. Efficiency: Any group member can store and share data files with others in the group by the cloud. User revocation can be achieved without involving the others, which means that the remaining users do not need to update their private keys.

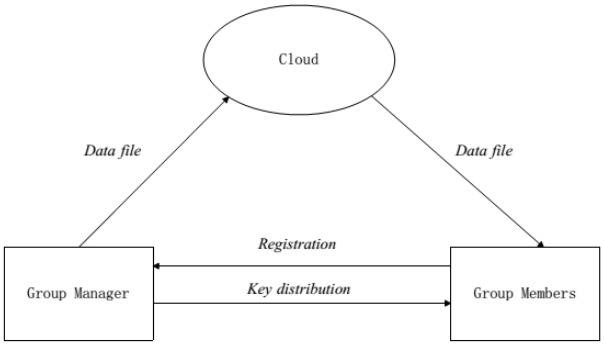


Fig 4.1 System Architecture

As illustrated in the above figure, the system model consists of three different entities: the cloud, a group manager and a large number of group members. The cloud, maintained by the cloud service providers, provides storage space for hosting data files in a pay-as-you-go manner. However, the cloud is untrusted since the cloud service providers are easily to become untrusted. Therefore, the cloud will try to learn the content of the stored data. Group manager takes charge of system parameters generation, user registration, and user revocation. In the practical applications, the group manager usually is the leader of the group. Therefore, we assume that the group manager is fully trusted by the other parties. Group members (are a set of registered users that will store their own data into the cloud and share them with others. I n the scheme, the group membership is dynamically changed, due to the new user registration and user revocation. We describe the main design goals of the proposed scheme including key distribution, data confidentiality, access control and efficiency.

6. RESULTS AND DISCUSSIONS

The developed system is a secure data-sharing scheme where users can achieve an effective and economical approach for data sharing among group members in the cloud with the characters of low maintenance and little management cost. Meanwhile, we must provide security guarantees for the sharing data files since they are outsourced. Unfortunately, because of the frequent change of the membership, sharing data while providing privacy preserving is still a challenging issue, especially for an untrusted cloud due to the collusion attack. Moreover, for existing schemes, the security of key distribution is based on the secure communication channel, however, to have such channel is a strong assumption and is difficult for practice.
The proposed system contains six modules - Cloud, Group Manager, Group Member, File Security, Group Signature, and User Revocation Module.

In the cloud module, we create a local Cloud and provide priced abundant storage services. The users can upload their data in the cloud. We develop this module, where the cloud storage can be made secure.

In the group manager module the group manager takes charge of the system parameters generation, User registration, User revocation, and Revealing the real identity of a dispute data owner.

In the Group Member module, Group members are a set of registered users that will store their private data into the cloud server and Share them with others in the group.

In the File Security module encrypting the data file.
Either the group manager or the data owner can delete file stored in the cloud. (i.e., the member who uploaded the file into the server).

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

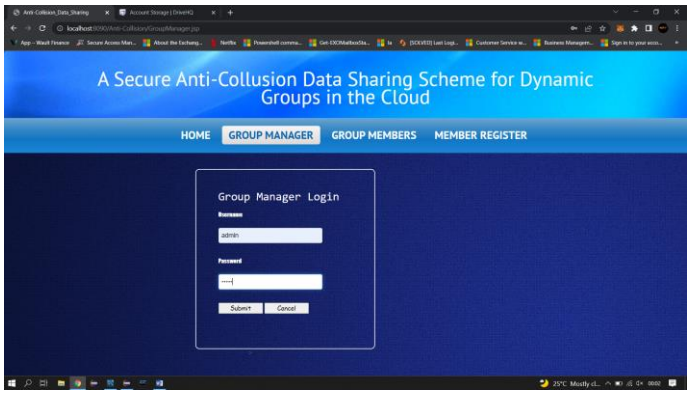
In the user revocation module is performed by the group manager via a public available revocation list (RL), based on which group members can encrypt their data

files and ensure the confidentiality against the revoked users.

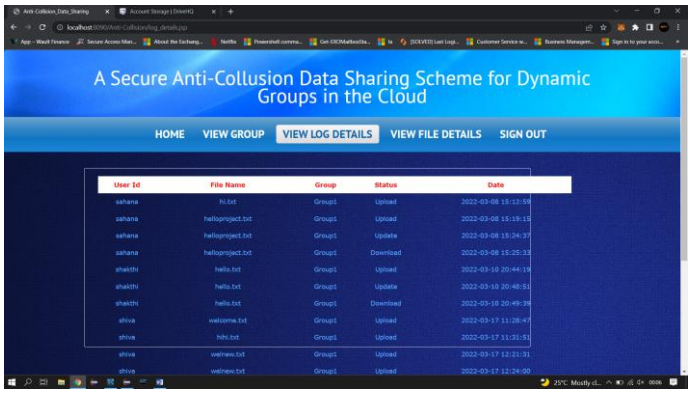
7. SCREENSHOTS

The welcome page displays the different modules that the user would like to use

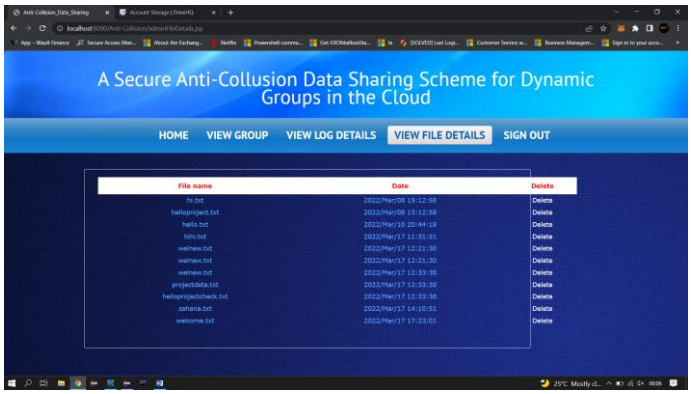
The Admin/ Group Manager enters the Username-admin, password-admin. This is the admin module where the admin can view the groups, view the log details and view the file details of the users present



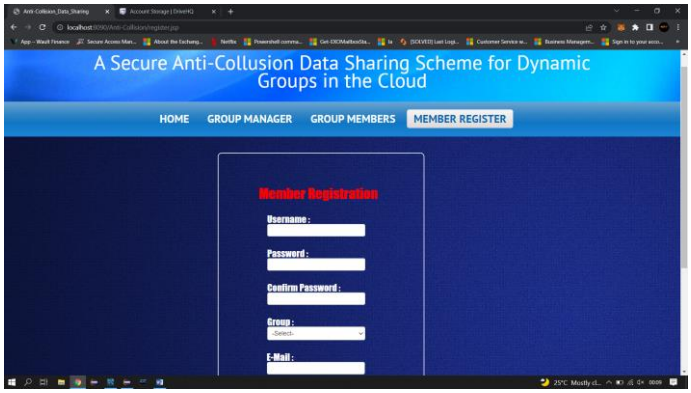
The view log details shows the user's ID, file name, which group the users belong to and status of files and the date



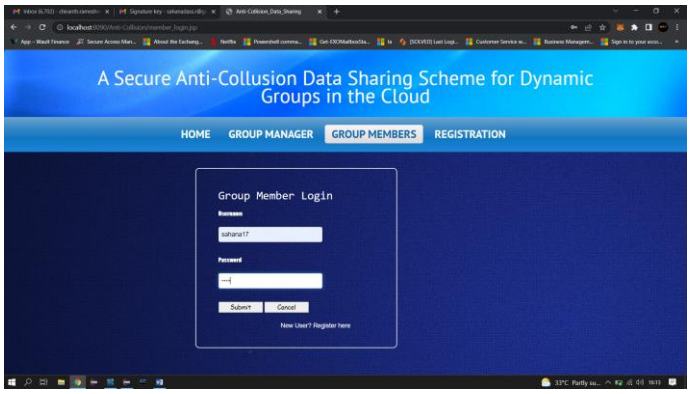
The view file details shows the files that were uploaded by the users and the admin has the sole rights to delete the files

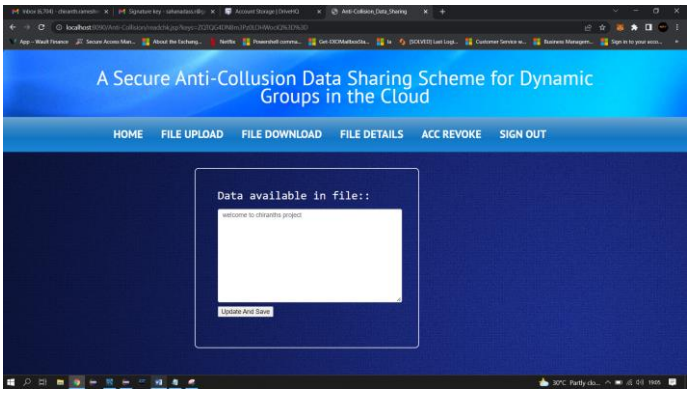


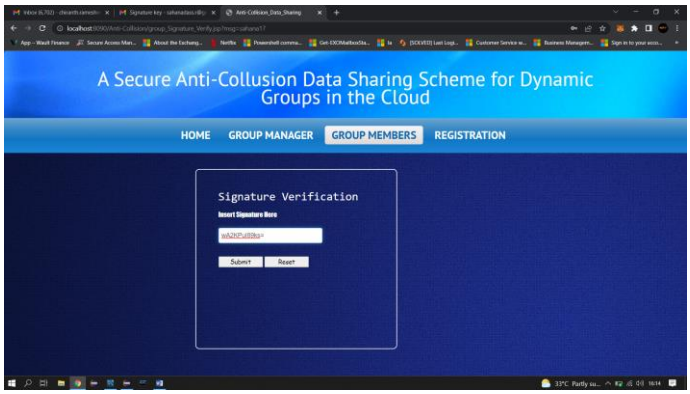
The new members can register themselves by entering the required fields, which creates a new account.



The member can now login to their account by entering their credentials. Member has to insert the security key that they received on their mail in order to login to their account







The Group member module as shown below the member has the access to the resources

The file uploaded has some content which can be updated and saved as well

8. CONCLUSION

To conclude, in this paper, we design a secure anti-collusion data-sharing scheme for dynamic groups in the cloud. In our scheme, the users can securely obtain their private keys from group manager with the help of the SMTP(Simple Mail Transfer Protocol) only with the help of the private key the user will be able to access the data. Our scheme is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated. Moreover, our scheme can achieve secure user revocation, the revoked users can not be able to get the original data files once they are revoked even if they conspire with the untrusted cloud.

9. ACKNOWLEDGEMENT

I should convey my real tendency and obligation to Dr M N Nachappa and Dr. Murugan R for undertaking facilitators for their effective steerage and consistent inspirations all through my assessment work. Their ideal bearing, absolute co-action and second discernment have made my work gainful.

10. REFERENCES

[1] P. Tzerefos, C. Smythe, I. Stergiou and S. Cvetkovic, "A comparative study of Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP) and X.400 Electronic Mail Protocols," Proceedings of 22nd Annual Conference on Local Computer Networks, 1997, pp. 545-554, doi: 10.1109/LCN.1997.631025.

[2] A. Syed, K. Purushotham and G. Shidaganti, "Cloud Storage Security Risks, Practices and Measures: A Review," 2020 IEEE International Conference for Innovation in Technology (INOCON), 2020, pp. 1-4, doi: 10.1109/INOCON50539.2020.9298281.

[3] Z. Zhu and R. Jiang, "A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud," in IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 1, pp. 40-50, 1 Jan. 2016, doi: 10.1109/TPDS.2015.2388446.

[4] K. V. R. Kumar and G. Murali, "Enhanced security for data sharing in clouds through policy and access control management," 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), 2017, pp. 3571-3574, doi: 10.1109/ICECDS.2017.8390126.

[5] K. Kapusta, H. Qiu and G. Memmi, "Poster Abstract: Secure Data Sharing by Means of Fragmentation, Encryption, and Dispersion," IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2019, pp. 1051-1052, doi: 10.1109/INFCOMW.2019.8845243.

[6] R. Krut and S. Cohen, "Service-oriented architectures and software product lines - putting both together," in SPLC, 2008, p. 383.

[7] R.S. Hassan, A. Nawaz, M.N. Lashari, & F. Zafar, "Effect of Customer Relationship Management on Customer Satisfaction", Procedia Economics and Finance 23 (2015) 563 - 567.

[8] Sheng, J. Being. “Active in Online Communications: Firm Responsiveness and Customer Engagement Behaviour”. Journal of Interactive Marketing, 46 (2016) , 40–51. 2019

[9] Serbest,S., Goksen,Y., Dogan,O., Tokdemir,A. “Design and Implementation of Help Desk System on the Effective Focus of Information System”. Procedia Economics and Finance. 2015, pp. 461 – 467

[10] W. Zhou, L. Tang, T. Li, L. Shwartz, and G. Y. Grabarnik, “Resolution recommendation for event tickets in service management,” in 2015 IFIP/IEEE International Symposium on Integrated Network Management(IM). IEEE, May 2015, pp. 287–295.