Mona: Secure Multi-Owner Data Sharing For Dynamic Groups In The Cloud

Akshay Desale[1] , Faiz Mapkar[2] , Ankit Loharaj[3] , Avinash Shrivas[4]
[1, 2, 3, 4] Dept of Computer
[1, 2, 3, 4] Vidyalankar Institute of Technology , Mumbai , India.

Abstract- *Cloud computing is a flexible and convenient manner for supplying offerings over the web which brings more than a few benefits for each the society and individuals. With the persona of low protection, cloud computing presents a cost-effective and efficient resolution for sharing crew resource amongst cloud customers. Cloud computing is getting developed daily and data is being centralized into remote cloud server for sharing, which raises a undertaking on easy methods to keep them personal as well as accessible. Sadly, sharing data in a multi-owner method while maintaining knowledge and identification privacy from an untrusted cloud remains to be a challenging quandary, because of the customary alternate of the membership. For that reason, the venture proposes a at ease multi-owner knowledge sharing scheme, named Mona, for dynamic businesses in the cloud. In Mona, a person is capable to share information with others within the staff with out revealing identification to the cloud. Additionally, Mona supports efficient user revocation and new person becoming a member of. More specially, efficient person revocation can be done through a public revocation record with out updating the personal keys of the remaining users, and new users can directly decrypt documents saved in the cloud earlier than their participation. With the aid of exploiting staff signature and dynamic broadcast encryption procedures, any cloud consumer can anonymously share data with others. Meanwhile, the storage overhead and encryption computation price of our scheme are independent with the quantity of revoked users. Moreover, we analyze the security of our scheme with rigorous proofs, and display the effectivity of our scheme by conducting experiments.*

Keywords- Access manage, Cloud Computing, information Sharing, Dynamic companies, privacy-keeping.

I. INTRODUCTION

Cloud computing is an internet based computing so the info can be always available to the patron and where via shared assets, application and information are supplied with the aid of the carrier vendors on demand. Cloud computing is an extraordinarily attractive atmosphere for business world in phrases of rate and delivering services. Cloud computing is a long dreamed imaginative and prescient of computing as a utility the place information owners can remotely store their data in a cloud to enjoy on-demand high excellent applications and services from a shared pool of configurable computing assets.

Advantages: -

1. 1.Place independent
2. 2.Effortless protection
3. 3.Secure storage and management
4. 4.High degree computing

Disadvantages: -

1. 1.Lack of control
2. 2.Safety and privacy
3. 3.Bigger operational rate
4. 4.Reliability

With cloud computing and storage, users are in a position to access and to share resources offered with the aid of cloud carrier vendors at a lessen marginal cost. With Dropbox, for example, information is stored in the cloud (operated by way of Amazon), and shared among a group of customers in a collaborative method. It is usual for users to wonder if their information remain intact over a chronic interval of time. The privacy of knowledge saved in the cloud can grow to be compromised. To protect the privateness of data in the cloud and to offer “peace of mind” to customer, it is pleasant to encrypt the info records and then add the encrypted knowledge into the cloud. Alas designing an efficient and cozy knowledge sharing scheme for organizations in the cloud will not be an convenient assignment because of following reasons. First, the identification of the information house owners need to be preserved. Second, the information owner should be competent to make use of the entire services supplied through the cloud storage provider supplier.

Many privacy techniques for data sharing on far off storage machines had been endorsed. In these models, the info owners retailer the encrypted data on untrusted faraway storage. After that they're going to share the respective decryption keys with the authorized users. This avoid the cloud provider providers and intruders to access the encrypted data, as they don't have the decrypting keys. Nonetheless, the new knowledge proprietor registration within the above said models exhibits the identity of the new information proprietor to the others in the team. The brand new data owner has to take permission from other knowledge house owners in the workforce earlier than producing a decrypting key. The proposed method identified the issues in the course of multi owner information sharing and proposed an effective protocol and cryptographic technique for solving drawbacks within the traditional procedure. It proposed an efficient and novel relaxed key protocol for team key iteration and utilising these key information owners can encrypt the files. Believe new person register into group the consumer don't need to contact the data owner throughout the downloading of files.

II. MOTIVATION

Up to now, to be able to continue information privacy, a basic resolution is to encrypt data records, after which upload the encrypted data into the cloud. Knowledge homeowners store the encrypted data records in untrusted storage and distribute the corresponding decryption keys only to approved customers. For this reason, unauthorized customers as well as storage servers are not able to be taught the content of the data files considering they've no expertise of the decryption keys. Nevertheless, the complexities of user participation and revocation in these schemes are linearly increasing with the quantity of knowledge homeowners and the quantity of revoked customers, respectively.

The venture is taken to be able to fully grasp the difficulties in designing an efficient and comfy knowledge sharing scheme for dynamic groups in the cloud in a multi-proprietor manner, its motive and design ambitions.

III. PROBLEM DEFINITION

Designing an effective and comfy data sharing scheme for agencies in the cloud shouldn't be an effortless assignment due to the next challenging problems:

- Identity privacy is one of the most enormous boundaries for the wide deployment of cloud computing. Without the assurance of identity privacy, users could also be unwilling to join in cloud computing programs seeing that their real identities would be easily disclosed to cloud vendors and at attackers.
- Then again, unconditional identification privacy could incur the abuse of privacy. For example, a misbehaved employees can deceive others within the enterprise by means of sharing false files with out being traceable.
- Only the workforce supervisor can store and modify information in the cloud.
- The changes of membership make secure data sharing particularly intricate and the difficulty of person revocation just isn't addressed.

Right here, we advise a cozy multi-proprietor data sharing scheme, named Mona, for dynamic organizations within the cloud. Utilising workforce signature and dynamic broadcast encryption techniques, any cloud consumer can anonymously share knowledge with others.

IV. SCOPE

The scope of this challenge limits to:

1. Process Initialization: The workforce manager takes charge of method initialization.
2. Person Registration: every authenticated group member fills registration kind with the intention to get exclusive key from team supervisor.
3. Consumer Revocation: consumer revocation is carried out by way of the team manager by way of a public on hand revocation list (RL) founded on which workforce participants can encrypt their information documents and be certain the confidentiality against the revoked users.
4. File generation: To retailer and share a knowledge file within the cloud.
5. File Deletion: File saved within the cloud can also be deleted by way of both the staff manager or the info owner (i.e., the member who uploaded the file into the server).
6. File access: To be trained the content material of a shared file.
7. Traceability: When a knowledge dispute occurs, the tracing operation is performed through the workforce supervisor to determine the real identification of the data owner.

V. PROPOSED SYSTEM

To acquire cozy information sharing for dynamic organizations in the cloud, we expect to mix the crew signature and dynamic broadcast encryption strategies. Exceptionally, the staff signature scheme allows users to anonymously use the cloud assets, and the dynamic broadcast encryption procedure allows for data house owners to soundly share their data records with others together with new joining customers.

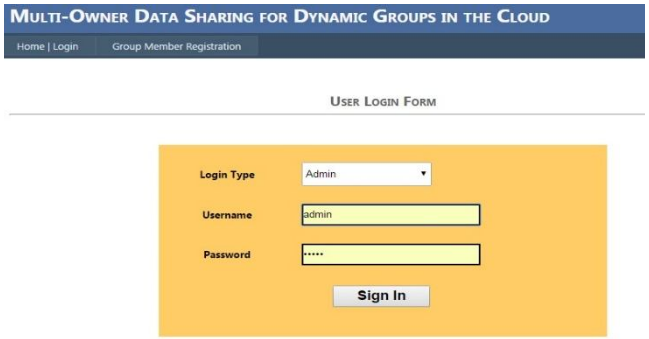
Alas, each user has to compute revocation parameters to defend the confidentiality from the revoked users in the dynamic broadcast encryption scheme, which outcome in that each the computation overhead of the encryption and the scale of the cipher text increase with the number of revoked customers.

To tackle this challenging limitation, we let the crew manager compute the revocation parameters and make the outcomes public available by migrating them into the cloud. Any such design can enormously lessen the computation overhead of customers to encrypt documents and the cipher textual content measurement. Principally, the computation overhead of users for encryption operations and the cipher text measurement is constant and unbiased of the revocation customers.

VI. IMPLEMENTATION

1. Admin Module

The main purpose of this module is to take charge of group manager generation. As per the requirement, Admin can create group manager account. Roles and responsibilities of Admin is to just create, update and view the details of group manager in the List of Group Manager. There are no more additional responsibilities to the Admin Entity.


MULTI-OWNER DATA SHARING FOR DYNAMIC GROUPS IN THE CLOUD
Home | Login
Group Member Registration

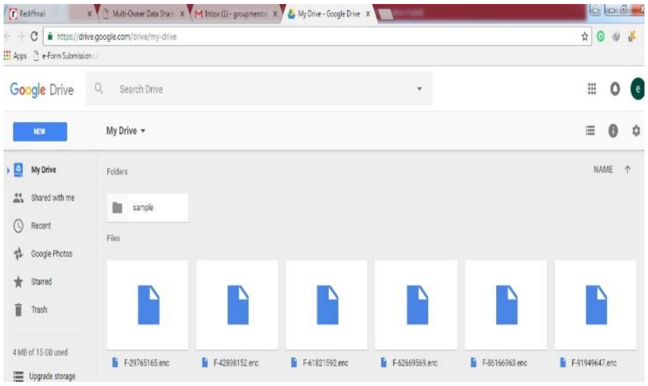
USER LOGIN FORM

Login Type: Admin ▾
Username: admin
Password: •••••

2. Cloud Module

In this module, we create a local Cloud and provide abundant storage services. The group members can upload their data in the cloud. We develop this module, where the cloud storage can be made secure. However, the cloud is not fully trusted by group members since the CSPs are very likely to be outside of the cloud users' trusted domain. Similarly, we assume that the cloud server is honest but curious.

That is, the cloud server will not maliciously delete or modify user data but will try to learn the content of the stored data and the identities of cloud users. Thus, we use cloud server [Google Drive] for file storage purpose and server account will be maintained by group manager so that the group members can utilize the service efficiently. The encrypted files are stored in the cloud server by group members. Group manager act as a mediator between cloud and group members. Server account is managed by group manager and also makes the server account available to the group manager.

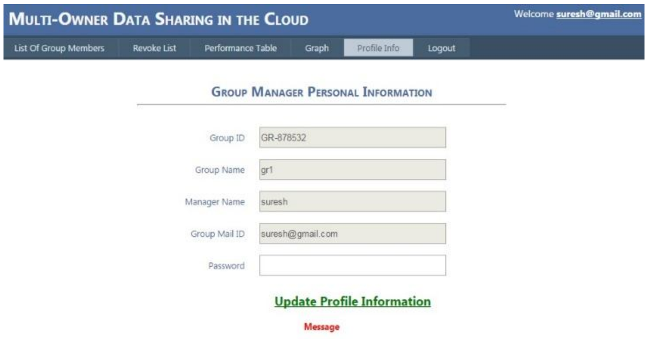


3. Group Manager Module

Group manager takes charge of following components:

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. And the group manager maintains the log of each and every process in the cloud. The group manager is responsible for user registration and also user revocation too. As soon as the group manager activates the registered user account, users are now allowed to login as well as the respective private key such as parameter X, A and B is distributed among the users.

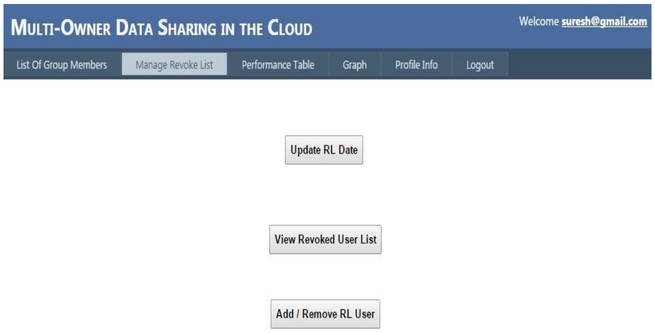


Group Manager Personal Information

Group ID: GR-878532
Group Name: gr1
Manager Name: suresh
Group Mail ID: suresh@gmail.com
Password:

4. User Revocation Module

User revocation 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. group manager can actually view the total number of revoked user list and if needed, group manager can change the decision by removing from revocation list. Additionally, group manager can also view the revoked time, member ID and user mail ID.



5. Group Member Module

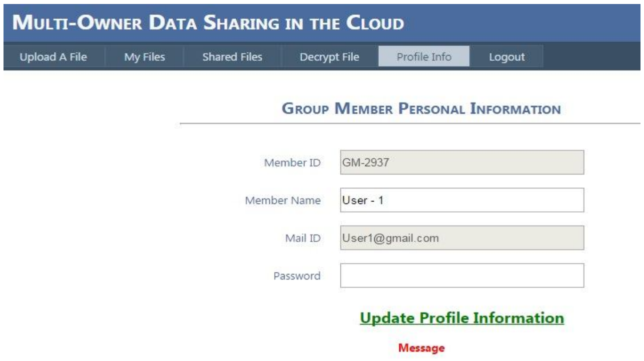
Group members are a set of registered user, they will store their private data into the cloud server and share them with others in the same group. Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company. A group member has the ownership of changing the files in the group. Group members in the group can download the files which are uploaded in their group and also modify it.

Registration**:** In this module, User has to register first, then only he/she has to access the data base.

Login**:** In this module, any of the above mentioned person have to login, they should login by giving their email and password. Data Owner uploads the file into cloud server.

Upload: The uploaded file will be in encrypted form; only registered user can decrypt it. Even CSP can only view the encrypted file form.

Download: The Registered users can download the file and can do updates. The modified file will be uploaded into cloud server by the user.



Group Member Personal Information

Member ID: GM-2937
Member Name: User - 1
Mail ID: User1@gmail.com
Password:

VII. CONCLUSION

Within the proposed system, a user is in a position to share information with others within the workforce without revealing identification privateness to the cloud. moreover, helps effective person revocation and new person joining. more especially, efficient user revocation can also be completed by means of a public revocation record without updating the personal keys of the rest usersAnd new users can straight decrypt files saved in the cloud earlier than their participation. moreover, the storage overhead and the encryption computation cost are consistent.

VIII. FUTURE WORK

Our undertaking has been developed in general by way of taking the example of the atmosphere of the manufacturer. We will lengthen our task to the fields akin to schooling, enjoyment, various social networks and different wider areas. For illustration, we can rent our assignment in the universities to maintain the data base of the pupils which can be used by means of the organizations of lecturers. Here lecturer turns into the crew member and the pinnacle of the division turns into the staff manager. Further enhancement within the safety of the info uploaded through the members can be achieved. We will also be aware of developing sub businesses within the organizations. We are able to pay attention to keeping identification privacy for its enhancement. Interplay between the crew manager and the workforce member must be increased.

REFERENCES

[1] Xuefeng Liu, Yuqing Zhang, Member, IEEE, 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] 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.

[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] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage,” Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.

[5] 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.

[6] The Pairing-Based Cryptography Library (PBC), http://crypto. stanford.edu/pbc/howto.html, 2013.

[7] 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.

[8] 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.

[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), pp. 89-98, 2006.