ISSN:0975-9646

Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud

T.Vijayalakshmi[#1], N.Suresh[#2]
[#]*Computer science and Engineering, QIS Institute of Technology*
Ongole, Andhra Pradesh, India

***Abstract*— Now a days cloud computing plays a key role for sharing group resource among their users. Due to the frequent changes of membership maintaining multi owner data is becoming a difficult task and also sharing of data in an un trusted cloud is also a major challenge. For that purpose we introduce the MONA for dynamic groups in the cloud and it supports for group signature and broadcast encryption techniques. So that any cloud user can share data with the others. Here the revocation list is also presented.**

Key Words-Cloud Computing, data sharing, dynamic groups, privacy maintenance, access control.

1.INTRODUCTION

Cloud computing is an internet based computing so the data will be always available to the client and where by shared resources, software and information are provided by the service providers on demand. It means in cloud computing is done by migrating local data management systems into cloud servers, users can enjoy high quality services and save significant investments on their local infrastructure. Cloud computing is very attractive environment for business world in terms of cost and providing services. Cloud computing is long dreamed vision of computing as a utility where data owners can remotely store their data in a cloud to enjoy on demand high quality applications and services from a shared pool of configurable computing resources.

Advantages and disadvantages of cloud computing
Advantages:-

- Location independent
- Easy maintenance
- Secure storage and management
- High level computing

Disadvantages:-

- Lack of control
- Security and privacy
- Higher operational cost
- Reliability

2.RELATED WORK

In 2003, Kallahalla proposed a system named PLUTUS enables the secure file sharing on the un trusted cloud servers by using the cryptographic storage system. In this method, the files are divided into the file groups and encrypting each group with a unique file block key. Now the data owner can share the file groups with the others by delivering the corresponding lock box keys, where the lock box key is used for encrypting the file-block keys. But this brings a heavy key distribution for the large amounts of file sharing and more additionally the file-block keys need to be updated every time when ever the user revocation occurs and the updated keys has to be distributed.

In 2003, the E.Goh and his team proposed a system named "sirius". In that the files stored on the untrusted server include two parts: file metadata and file data. In the file meta data it include a series of encrypted key blocks and each one is encrypted by the public key of the authorized users. Here also the user revocation is an intractable issue for the large-scale file sharing. Since every time the file's meta data also need to be updated. In the next version , the NNL construction is used for the efficient key revocation .But in this also whenever a new user joins in the group, there is no need to recomputed the private keys of the every user.

In 2005, ateniese et.al proposed the proxy re encryptions for the secure distributed storage. Here in this the concept of encryption computation overhead increases with the data sharing rate. In this the data owner encrypts the data with the two types of keys like unique and symmetric content keys. These two keys are further encrypted by a master public key. Here for the access control, the server uses proxy cryptography to directly re encrypt the keys with the master public key granted user's public key. But when any revoked users can be launched they will be able to learn the decryption keys.

In 2010,Yu.et.al proposed a scalable and fine grained data access control scheme in the cloud computing by using the KP-ABE technique. In this scheme, the data owners encrypt the file with a rand key where this random key is further encrypted with a group of attributes y using the KP-ABE and the respected secret keys to the authorized users, then the user can only decrypt the cipher text if the data file attributes match with the access structure. To achieve the user revocation the cloud servers takes the responsibility from manager of the tasks such as file re encryption and the secret key updates. Here in this scenario, the single owner manner may create the problem with the implementation of applications where all the users can share data with the others.

In 2010 the Lu.et.al proposed the secure provenance scheme. In this they implemented the group signatures and the cipher text policy ABE techniques. In this scheme the system is set with a single attribute. In this method the user gets two keys after the registration. The two keys are group signature key and the remaining users in the same group can decrypt the data with their group signature key for the privacy preserving and traceability. But in this scheme the user revocation is not presented.

By Observing all this analysis we have a greater challenging issue that is how we can securely share data with the others by the multiple-owner manner for the dynamic groups in the un trusted cloud along with

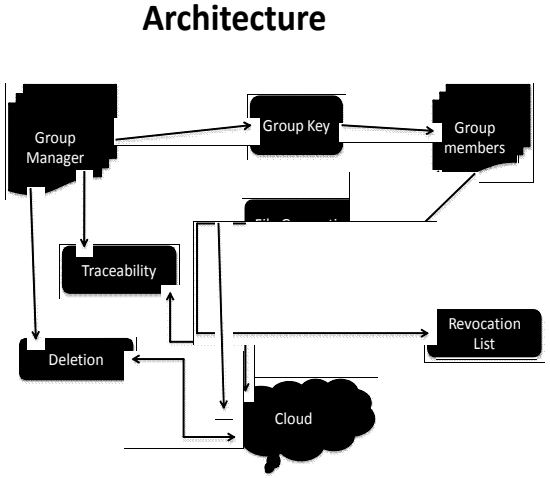
preserving identity privacy. Now in this project, we are proposing a new protocol MONA, for secure data sharing in the cloud computing. Here the MONA offers some unique features when compared with the others. The unique features are as follows:

1. Any group member can share data files with others and can also store the data files in the cloud.
2. In this the number of revoked users is independent with the complexity of encryption and also the size of cipher texts.
3. There is no need of updating the private keys of the remaining users whenever the user revocation occurs
4. The new users can directly access the files that are stored n the cloud without their participation.
5. Here we are including the backup group manager for improving the reliability and scalability.

3. CONCEPT OF MONA

Maintaining the integrity of data is not an easy task. It plays a vital role in the establishment of trust between the service provider and the data subject. Although the new technology as a promising service platform for the internet, the new data storage paradigm in cloud brings some more challenging issues which influence the security and performance of the overall system. In those issues one of the biggest concerns is data integrity verification at un trusted servers. In this for saving money and storage space service providers might neglect to delete/keep the rarely accessed files which belongs to a ordinary client. So the periodical verifications must be an important task. For preserving data privacy the general concept is data encryption and then uploads the encrypted data into the cloud. Still some clients are not able to upload and delete files securely and also for accessing the data efficiently. Now we are proposing the scheme which solves the above mentioned problems. Here in this system clients can efficiently access, add or delete the data from the cloud and also a multi-owner manner is presented. That is anyone of the cloud user with the access permission can efficiently access/modify the data at any time.

4.ARCHITECTURE EXPLANATION



Here in this architecture there are 3 main modules. They are group manager, group members and cloud group. Here the group anger generates the group key and it was distributed to the group members after the successful login. Now the group member can generate a file and can access files which are connected to the cloud that means we store information in the cloud. Here the revocation list is also presented where the revocation of users is common in the organization. Here the group manager has traceability and deletion options. Traceability offers the group manager can see the accessing of all the members details at any time. Deletion offers to delete any file at any time. These two options are linked with the cloud which is further related to the cloud.

Algorithms Used:-

- Signature Generation - Here we are generating the group signature and file generation by using this signature generation method. In this group signature and file key generation can be done by using the Triple DES encryption process.
- Signature Verification - Here we have to verify the group signature key and file key's with the Triple DES decryption process.
- Revocation Verification - Here we use to check the user revocation which is used for the verification of user's list.
-

1. Signature Generation

Here we encrypt the input data by using the Triple DES algorithm. The algorithm steps are as follows:

1.Let us consider private key (A,x) and system parameters as (P,U,V,H,W) where data is referred as M.

2.Select random numbers α, β , r_α ,r_β, r_x,r_y,$r_{\delta 1}$,$r_{\delta 2} \in z_q^*$.

3.Set $\delta 1 = x\alpha$ and $\delta 2 = x\beta$.

4.Now we compute the following values as,

$$\begin{cases} T_1 = \alpha \cdot U \\ T_2 = \beta \cdot V \\ T_3 = A_i + (\alpha + \beta) \cdot H \\ R_1 = r_\alpha \cdot U \\ R_2 = r_\beta \cdot V \\ R_3 = e(T_3, P)^{r_x} e(H, W)^{-r_\alpha - r_\beta} e(H, P)^{-r_{\delta_1} - r_{\delta_2}} \\ R_4 = r_x \cdot T_1 - r_{\delta_1} \cdot U \\ R_5 = r_x \cdot T_2 - r_{\delta_2} \cdot V \end{cases}$$

5.The first encryption set of values are as follows set $C=f(M,T_1,T_2,T_3,R_1,R_2,R_3,R_4,R_5)$.

6.Now we consider another set of random numbers for further encryption process as $(C_\alpha, C_\beta, C_x, C_{\delta 1}, C_{\delta 2})$.

$$\begin{cases} s_\alpha = r_\alpha + c\alpha \\ s_\beta = r_\beta + c\beta \\ s_x = r_x + cx \\ s_{\delta_1} = r_{\delta_1} + c\delta_1 \\ s_{\delta_2} = r_{\delta_2} + c\delta_2 \end{cases}$$

7.After the complete encryption process the result is $\sigma=(T_1,T_2,T_3,C,S_\alpha,S_\beta,S_x,S_{\delta 1},S_{\delta 2})$.

2. Signature Verification

In signature verification process here the decryption process is used.

1. Here the input is the encrypted form of the data which was generated in the Signature generation process. The input parameters are System parameters(P,U,V,H,W),M and the signature $\sigma=(T_1,T_2,T_3,C,S_\alpha,S_\beta,S_x,S_{\delta 1},S_{\delta 2})$.

2.Here we compute the following values

$$\begin{cases} \tilde{R}_1 = s_\alpha \cdot U - c \cdot T_1 \\ \tilde{R}_2 = s_\beta \cdot V - c \cdot T_2 \\ \tilde{R}_3 = (\dfrac{e(T_3,W)}{e(P,P)})^c e(T_3,P)^{s_x} e(H,W)^{-s_\alpha - s_\beta} \\ \qquad\qquad e(H,P)^{-s_{\delta_1} - s_{\delta_2}} \\ \tilde{R}_4 = s_x \cdot T_1 - s_{\delta_1} \cdot U \\ \tilde{R}_5 = s_x \cdot T_2 - s_{\delta_2} \cdot V \end{cases}$$

3.After completing the generation of variables. We have to calculate the following function $f(M,T_1,T_2,T_3,R_1',R_2',R_3',R_4',R_5')$.

4.Here if the generated function is equals to the c (first encrypted result in encryption process) then it returns the result as true otherwise it will show the result as false.

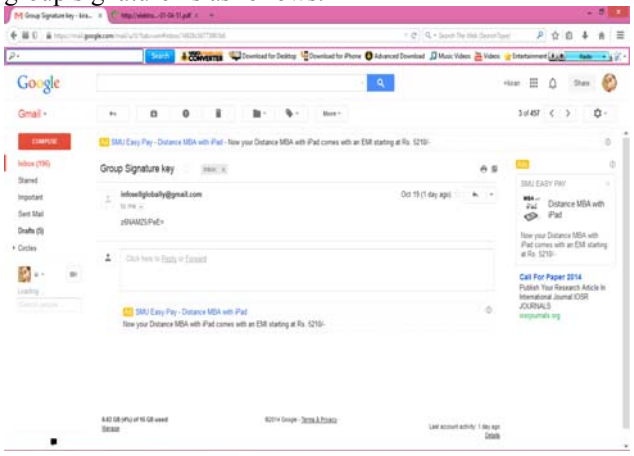
3. Revocation Verification

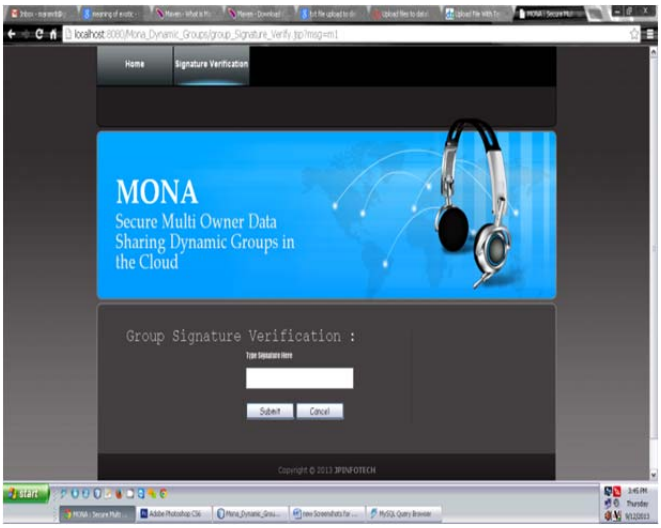
Here the revocation is verified by using the following steps.

1. Here the input parameters are (H_0,H_1,H_2) and the group signature $\sigma=(T_1,T_2,T_3,C,S_\alpha,S_\beta,S_x,S_{\delta 1},S_{\delta 2})$ and a set of revocation keys $A_1,....,A_r$
2. Here we set the temp file with the following set *temp*=$e(T_1,H_1)e(T_2,H_2)$
3. for i =1 to n if $e(T_3-A_i,H_0)$=*temp*
4. Here if we get the two values are equal it returns a valid message and otherwise it returns invalid message.

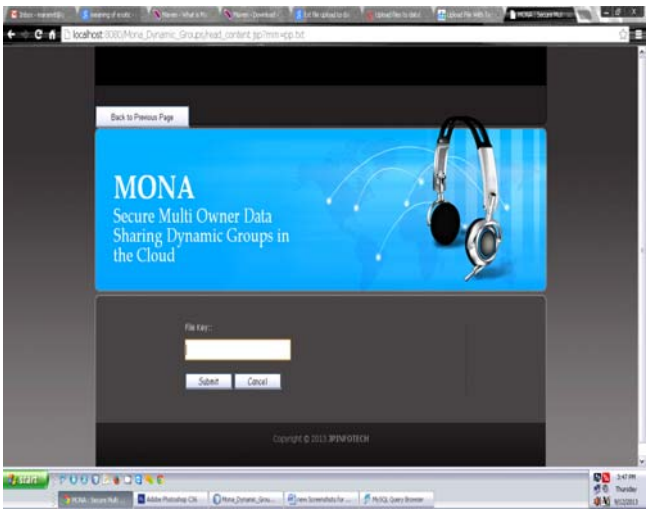
EXPERIMENTAL RESULTS:-

In this project whenever the group member is registering with the group ,they have to be give their mail id's also in the details list.Basing on this when the group manager accepts the request of the group member they will send the group signature to their id's.Each and every time when the group member login to the group they have enter the group signature also.The screen where they have to enter the group signature is as follows.





Here when the user uploads a file in the group, the file key is generated. This key is very important for updating, downloading and viewing the file. The following is the screenshot for entering the file key.



5. CONCLUSION AND FUTURE WORK

In this paper, we design a secure data sharing scheme, Mona, for dynamic groups in a un trusted cloud. In Mona, a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, Mona 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 desired security requirements and guarantees efficiency as well. But here whenever the file is updated by the group members the file key is same after the updating also.In future the file key updations are also important for improving the security.

REFERENCES

[1] 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.

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

[3] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[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.

[10] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.