ISSN:0975-9646

M.Kavya et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 6926-6928

Privacy Preserving Data Sharing in Multi Groups

M.Kavya[1], M.V. Jagannatha Reddy[2]

[1 2] *Department of Computer Science and Engineering*
[1] *M.Tech Student, MITS Engineering College, JNTUA*
[2] *Associate Professor, MITS Engineering College, JNTUA*

Abstract-Cloud computing afford competent solution for distribute resource between multi users and multi groups. Unfortunately, information may shared by multi-user and multi-groups while preserving information, suitable normal change of the membership and unique privacy from un-trusted cloud and also data share only within the group is a difficult problem. In this work proposed that the data users can share the information from one group to another group by generating group signature on massages simply with a general secret key, it is also possible to reach identity privacy on messages. Here, a homomorphic authenticable group signature supports. Thus, we can still save communication and computation cost for users.

Keywords: Cloud computing, data sharing, group signature, homomorphism, access control, dynamic groups.

1. INTRODUCTION

Cloud computing is a type of computing that relies on sharing computing resources [1] rather than having local servers or personal devices to handle applications. The term Cloud refers to a Network or Internet. It offers online data storage, infrastructure and application. In this, the cloud service providers such as Amazon are delivered to cloud users with facilitate of datacenters. By using cloud users enjoy to access data, upload data and to share data. In any organization allow staffs in the same department or group is to access data, upload data and to share data files in the cloud. However, it causes a major risk to the stored user data files. The cloud servers are maintained by cloud providers are not completely trust by users when data is stored in the cloud sometimes the data be sensitive and private, such as company strategy. To provide privacy preserving user's data in the cloud the major solution is to encrypt [2] the data before uploading file into cloud. The others have no knowledge to decrypt the data. There are many security methods for information sharing on untrusted servers [3], [4], [5]. Here, the three entities are the cloud, the group manager and the group members [6]. The group manager allows registering group members, after registration key distributed by group manager. Group manager are highly recommended to store data into Cloud. The encrypt data can be stored and access by group members. Group manager takes charge of system parameter generation, user registration, user revocation, and revealing the real identity of a dispute data owner. Consider, that the group manager act as an admin and also the group members act as a staffs in organization. Here, we imagine that the group manager is completely trusted by other parties. The number of registered users joins in the group. The group manager distributes the secret key thus the group members can access data, store data and share data with others in the group. Note that the group members change dynamically due to new member's registration and user revocation in the group. When multiple data owners are involved, the aspects of membership and data sharing need to be addressed. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously distribute information with others. In this technique data can be uploaded in to the server after the encryption of the content by the secret group key. When new member joined in the group, new granted users can directly decrypt data files uploaded without contacting with data owners. Here, the major drawback that the data sharing only in the same group. In organizations have not only a single group there are number of groups. Here, to solve the issue by privacy preserving data sharing in multi groups. The group manager maintains the user registration, key distribution and maintain revocation list. For each group have the same secret key. When new user registered in group, group manager activate the user and then distribute the key personally. Here, a homomorphic authenticable group signature [7] supports to share data from one group to another group by generating group signature on messages only with a common secret key; it is also possible to achieve identity privacy on messages. Thus, we can still save communication and computation cost for users.

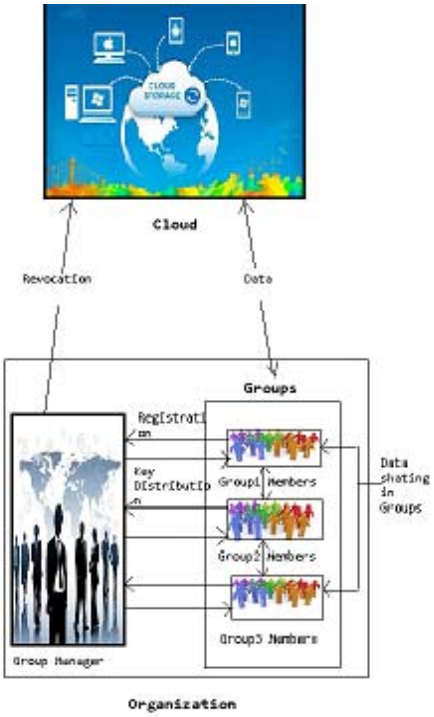
2. RELATED WORK

In this a secure multi-users information sharing scheme, name as Mona, for dynamic groups in the cloud. By means of active broadcast encryption and group signature techniques. Any member within the group can save and distribute information with other through the cloud. The group member revocation is achieved with no updating the secret key of the outstanding members. A new member is able to directly decrypt the records stored in the cloud after his membership no needs to contact the data-owner.

3. PROPOSED ARCHITECTURE

3.1. Proposed System

In this paper, we proposed a privacy preserving data sharing in multi groups. In dynamic groups the data can be shared by group members within the group or one group to another group. Entire group users produce signatures on messages only with a regular secret key. It is also possible to reach unique privacy on messages. Here, a homomorphic authenticable group signature supports. Thus, we can still save communication and computation cost for users.



4. MODULES AND IMPLEMENTATION

4.1. Modules

4.1.1. Authentication:

In this module User want to give the database to admin all the registration processes are done by an admin. After the registration process completed User can get the authentication permission, by using password and username login website. If the user enters a valid password and username then they will be approved to access data. If the client enter invalid password and username that client will be measured as unauthorized user and denied access to that client.

4.1.2. Group Manager:

Group manager takes charge of followings,

1. System parameters generation,
2. User registration,
3. User revocation, and
4. Revealing the real identity of a dispute data owner.

Subsequently, we expect that the group manager is completely trusted than the other parties. The Group manager is the admin. The group manager has the logs details of each and every process in the cloud. The group manager is responsible for user registration and also user revocation too. Then the authorized users pay for the cloud server and get the allocation space. And the Authorized person stores secure data to cloud. Get the access control and then provide the group members.

4.1.3. Store the data into cloud:

In this module, the authorized person can access information from cloud server, by uploading data, access data and distribute information with others in the group or from one group to another group that the data will be access the registration user only.

4.1.4 Maintain Revocation List:

The cloud storage gets the resignation user details from the company and maintains the revocation list. Because identify the unauthorized users and they can't contact the cloud data on any point, and revoked users also unable to access data once the group user revoked.

4.1.5. Maintain Access Control List:

The cloud storage gets the registration user details from the company and maintains the revocation list. Because identify who are the authorized users and who can access the cloud resource at any time.

4.1.6. New User:

In this module user will register and get the access control key from the managers, so they are access the cloud directly.

4.1.7. Group Signature Module:

A group Signature method allow when the group member to sign messages to keep the identity secret from verifiers. Here, only the group manager can expose the identity of the signature's originator when a dispute occurs, which is denote as traceability.

4.1.8. File Sharing:

In this module, the registered users in the group share data to other group users.

4.2 Implementation:

In dynamic groups the data can be shared by group members within the group or one group to another group. Entire group users produce signatures on messages only with a regular secret key. It is also possible to reach unique privacy on messages. Here, a homomorphic authenticable group signature supports. Homomorphic is nothing but homomorphism. Homomorphism is a basically a map from one group to another group. If we have two groups G and G' then we define the function Φ: G→G' to be a homomorphism, if bijective then it is an isomorphism.

Here homomorphic authenticable group signature contains algorithms: **KeyGen**, **Join**, **Sign**, **Verify** and **Open**. The group manager provides cloud to the groups and allows the group members after registration. The group manager generates a common secret key for each group. A group member can sign messages using his private and the group public key. By using cloud users enjoy to access data, upload data and to share data. A verifier is used to check the correctness of messages using the group public key, but he can't expose the identity of the signer, only the group manager can expose the identity of the signer message. The group manager can also add a private key for any group member and also add this member into group member list.

5. CONCLUSION

In this thesis, we design a privacy preserving data sharing in multi-groups. Here, a user can distribute information with others in the group and also can share data from one group to other group, user revocation and new user joining is supports. Group manager maintain revocation list without knowing the secret keys of the remaining users. Data sharing is achieved in multi-groups by generating group signature on messages only with a common secret key. It is also possible to achieve identity privacy on messages. Thus, we can still save communication and computation cost for users.

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] 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.

[4] 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.

[5] 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.

[6] Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud,"

[7] Rosario Gennaro, Daniel Wichsy, "Fully Homomorphic Message Authenticators,"