International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 07 | July-2017 www.irjet.net p-ISSN: 2395-0072

AN EFFICIENT SCHEME FOR DATA SHARING AMONG DYNAMIC CLOUD MEMBERS

Mahejuba Soudagar[1], Rajashekhar D. Salagar[2]

[1]M.Tech Student, Department of Computer Science and Engineering, BLDEA's V.P. Dr.P.G.Halakatti College of Engineering & Technology Vijayapur, Karnataka, India
[2]Assistant Professor, Department of Computer Science and Engineering, BLDEA's V.P. Dr.P.G.Halakatti College of Engineering & Technology Vijayapur, Karnataka, India

---

Abstract – *Cloud Computing, has the properties of sharing information and the cost of management maintainence is less. Cloud Computing provides a high usage of resource. Sharing the data along with giving privacy is a challenging issue because of the frequent change in membership. In this research work, we propose a scheme for sharing data which is secure for dynamic members. First, key distribution method is proposed without any communication channels, and the Group Managers provide keys to users. Second, fine grained access control can be achieved, cloud data can be used by any user within the cloud and users who are revoked cannot access the cloud. Third, the scheme is protected from collusion attack, i.e revoked users after they are revoked won't be able to get the original data even if they join with the third party cloud.*

***Key Words*: key distribution, privacy-preserving, fine grained access control (FGAC).**

1. INTRODUCTION

Cloud Computing, has the properties of sharing information and the cost of management maintenance is less. Cloud Computing provides a high usage of resource, It is the next most important step in the evolution of information technology, which includes many of and new and already existing technologies such as SOAs(Service Oriented Architecture) and virtualization. However, data shared in cloud usually contains personal information (such as personal profile, financial data, health records, etc.) and hence it must be well secured. Since we obtain data from third party servers, which is sensitive to cloud providers so security is the main constraint. A common method to maintain data privacy is encrypting data files before uploading it to cloud[2]. However, it is difficult to have such a scheme, especially for groups in the cloud.

A secured storage system which provides cryptography is used which gives a data sharing scheme on untrustworthy servers which is based on some techniques which includes encryption that is encryption is performed on separate single file group using file block key, and dividing the data files into separate file groups. But for revocation of users the keys of file-block should be distributed and updated. The complexities of user revocation and participation in these schemes are increasing with the number of revoked users and the data owners

These are the main offerings of our scheme:

1) This scheme gives a secure method of key distribution without using any secure channels. The registered users here obtain their private keys without using any certificate authorities securely from the group managers

2) Fine-grained access control can be achieved using this scheme, also any registered user present in the group can use the cloud resource using the group user list and the users who are revoked won't be able to get the data from cloud after they are revoked.

3) The main benefit of this scheme is that data is secure from collusion attack also the data sharing process is safe and secure. Once any user is revoked he cannot obtain the originally existing data file even if they join hands with third party servers.

4) Dynamic groups can be handled efficiently by our scheme, so whenever any user gets added in group or a user is revoked who has already joined, other user's private keys need not be computed and updated again.

2. LITERATURE SURVEY

A. Survey on: Cryptographic Cloud Storage: We look into the difficulty of constructing a service of secure cloud storage on the peak of public cloud architecture where client does not trust the cloud service provider. Cloud storage can be grouped into two types as private and public cloud [1].The customer owns the private cloud and only trusted bodies have access to the private cloud. The cloud service provider owns the public cloud where data is out of control and could be attacked by third parties.

B. Survey on: Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage: In 1998, Blaze, Bloomer, and Strauss (BBS) proposed an application called atomic proxy re-encryption, in which a semi-trusted proxy converts a ciphertext for Alice into a ciphertext for Bob without seeing the underlying plaintext. Proxy re-encryption[3] allows a proxy to transform a ciphertext computed under Alice's public key into one that can be opened by Bob's secret key, but this method is not secure[2]. The primary advantage of our schemes is that they are

unidirectional (i.e., Alice can delegate to Bob without Bob having to delegate to her) and do not require delegators to reveal all of their secret key to anyone – or even interact with the delegate – in order to allow a proxy to re-encrypt their ciphertexts.

C. Survey on: Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud: Sharing data in a multi-owner way while preserving data and from an untrusted cloud is still a challenging issue, mainly due to the frequent change of the membership. To preserve data privacy, a simple solution is encrypting data files, and then uploading the encrypted data into the cloud. Thus to achieve the reliable and scalable in MONA[4], in this paper we are presenting new framework for MONA. In this method we are also presenting how to manage the risks like failure of group manager by increasing the number of backup group manager, hanging of group manager in case number of requests more by sharing the workload in multiple group managers.

3. EXISTING SYSTEM

The existing methods to retrieve the fine grain data access control of key policy attribute is based on "encryption, proxy re-encryption and lazy re-encryption [9]". It does not reveal any information about the data. But any group member can utilize the cloud service for storing and sharing data that may hide the implementation of applications. One method is to provide group signatures and encryption methods for a secure scheme. After registration every user will get two keys one for encryption and other for decryption which is attribute key[5]. A secure way of using encrypted file is by role based encryption algorithms. This scheme is efficient scheme in terms of storage for user revocation that combines encryption with role based access control policies. However verification of users are not taken into view. In the proposed system every user gets verified by the cloud admin.

3.1 Disadvantage in existing system:

- A secure and efficient data sharing scheme is difficult to design.
- Key distribution overhead is large.
- The verifications of users are not done so it leads to collusion attack
- There is a weak protection of commitment in the stage of identity token. So it is unsecure.

4. THE PROPOSED SCHEME

4.1 Preliminaries

1)(Basic Diffe-Hellman Problem (BDHP) Assumption [6]): Specified base point P and a value γ € It is easy to calculate γ.P. However, given P,γ.P, it is infeasible to calculate γ since of the discrete algorithm problem.

2)(Decisional Diffie-Hellman Problem (DDHP) Assumption [7]):

Notation	Description
IDEi	the identity of user i
IDdatai	the identity of data i
qk	the public key of the user
tk	the private that Needs to be negotiated with the group manager
KEY=(xi,Ai,B)	the private key which is Distributed to the user from the Group manger and used for data Sharing
base point Q and $aQ,(a+b)Q$	is infeasible to compute b Q.

Definition 3 (Weak Bilinear Diffie-Hellman Exponent [8])

Encpk(): Symmetric encryption algorithm used in the encryption key k
ASENC(): Asymmetric encryption Algorithm used in the encryption key ULI group user list DLI data list[6]

4.2 ALGORITHM/TECHNIQUE USED:

Elliptic Curve Cryptography (ECC): was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington) as an alternative mechanism for implementing public-key cryptography.

The equation of an elliptic curve is given as, $\mathbf{y^2 = x^3 + ax + b}$

Few terms that will be used

E -> Elliptic Curve
P -> Point on the Curve
N -> Maximum limit (Prime number)

Key Generation: Key generation creates both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt using its private key. Now, we have to select a number 'd' within the range of 'n'.

Using the following equation we can generate the public key **Q = d * P**.

d = The random number that we have selected within the range of (1 to n-1). P is the point on the curve. 'Q' is the public key and 'd' is the private key.

1) Encryption: Let 'm' be the message that we are transferring. We should represent this on the curve. This has in-depth implementation details. All the advance research on ECC is done by a company called certicom. Consider *'m'* has the point *'M'* on the curve *'E'*. Randomly select 'k' from [1 – (n-1)].

Two cipher texts gets generated let it be **C1** and **C2**. **C1 = k*P** and **C2 = M + k*Q**. C1 and C2 are sent.

2) Decryption: We have to get back the message 'm' that was sent to us, **M = C2 – d * C1**

M is the original message that we have sent.

4.3 SYSTEM ARCHITECTURE:

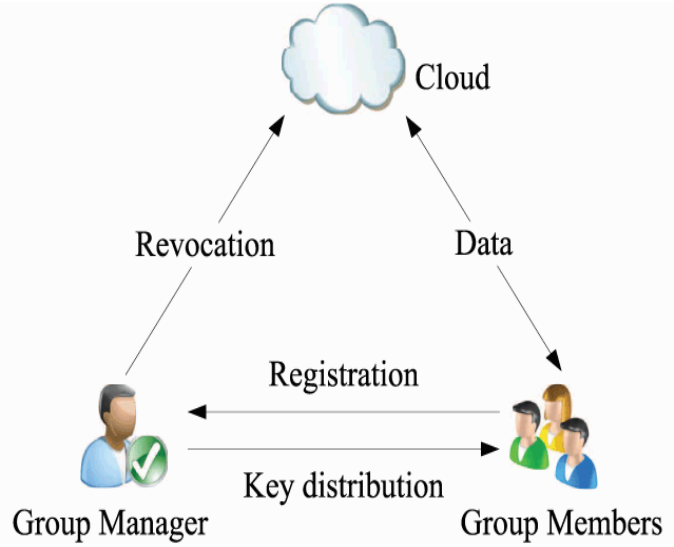

Fig -1: System Architecture

Shown in Fig. 1 above, there are 3 different entities included under the system model: the cloud, a group manager and many group members.

- **The cloud** It is the storage space available to the users on payment basis. It is maintained by the CSP. This becomes untrusted since CSP can be easily untrusted.
- **Group manager** is the one who has the authority of new user registration with the group and user revocation. He is the owner of the group so he is fully trustable.
- **Group members** or group (users) are the one that are registered by group manager. He can store their own data into the cloud and share them with other cloud member. Due to the new user registration and user revocation, the group membership varies vigorously.

4.4 Design Goals

Important design goals of our scheme are:

1) **Key distribution:** The users can get their private keys from the group manager securely. This is key distributions which do not need any certificates authorities or channel. In other systems a secure communication channel is required

2) **Access control:** Access control includes three main points. First, Members within the group can utilize the resources provided by cloud for storing and sharing data. Second, the users who are not authorized wont be able to utilize the resources of cloud. The revoked users also cannot use resources after being revoked

3) **Data confidentiality:** Data confidentiality means that unauthorized users including the cloud should not be able to learn information stored in cloud. However preserving the data confidentiality is a challenging issue for dynamic groups. Revoked users cannot decrypt the data after the revocation.

4) **Efficiency**: Main requirement of efficiency is that any group member can save the data files or share the data files with other group members of the cloud. Also here it is very easy to revoke users without informing others that is users need not update their keys.

5. ADVANTAGES

- The cost is not dependent on the number of the revoked users. Because file uploads cost computation is dependent on two signature verifications. These signature verifications are irrelevant to number of users revoked. In RBAC scheme the cost of computation is small because communication verification is not concerned.
- In our scheme, securely the users can get their private keys from group manager Certificate Authorities. Also, our scheme can maintain dynamic groups efficiently, whenever new users connect to the group, the other users' private keys need not to be recalculated and updated.

6. CONCLUSION

We have proposed a secure anti-collusion scheme for data sharing among dynamic groups in the cloud which is an efficient method. Here in this scheme, users can get hold of their private keys securely from group manager, secure communication channels and certificate Authorities. Our scheme also supports dynamic groups very efficiently, the private keys of the other users need not to be computed again and updated when a new user register in the group or an existing user is exited from the group. However, our

scheme achieves secure user revocation, the revoked users cannot obtain the original data after they are removed or exited even if they joins with the untrusted 3rd parties.

REFERENCES

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

[2] 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.

[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] X. Liu, Y. Zhang, B. Wang, and J. Yang, "Mona: Secure multiowner data sharing for dynamic groups in the cloud," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1182–1191, Jun. 2013.

[5] Z. Zhu, Z. Jiang, and R. Jiang, "The attack on mona: Secure multiowner data sharing for dynamic groups in the cloud," in Proc. Int. Conf. Inf. Sci. Cloud Comput., Dec. 7, 2013, pp. 185–189.

[6] B. Den Boer, "Diffie–Hellman is as strong as discrete log for certain primes," in Proc. Adv. Cryptol., 1988, p. 530.

[7] D. Boneh, X. Boyen, and H. Shacham, "Short group signature," in Proc. Int. Cryptology Conf. Adv. Cryptology, 2004, pp. 41–55.

[8] D. Boneh, X. Boyen, and E. Goh, "Hierarchical identity based encryption with constant size ciphertext," in Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2005, pp. 440–456.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.z