Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 5, May 2016, pg.690 – 696

Secure, Efficient Data Sharing For Dynamic Groups among Multiple Owners in Cloud with Anonymous Authentication

Rameshwar Indoriya[1], Navnath Shingade[2]

[1]Dept. of Computer Science & Engineering, Aurangabad College of Engineering, Aurangabad, Maharashtra

[2]Dept. of Computer Science & Engineering, Aurangabad College of Engineering, Aurangabad, Maharashtra

[1] rameshwarindoriya@gmail.com; [2] navnath.shingade@gmail.com

Abstract— Cloud computing is nothing but delivering applications as services over internet and these services are provided by combination of hardware's and software's of data center's and these services as Saas, Paas, Iaas etc. cloud computing commonly describe as "converting capital expenses into operating expenses (CapEx to OpEx)".Cloud computing provide ability to store data in cloud and share that valuable data to multiple authorized users. It also provides economical and efficient solution for sharing group resources among multiple cloud users. Sharing data among multiple users' lights on defensive of data and identity privacy of users from untrusted cloud is still challenging problem. Encrypting documents with different keys using public key cryptosystem such as Attribute based encryption (ABE) and Proxy re-encryption has some weaknesses. It can't efficiently handles adding or revoking users or identity attributes. In this paper we proposed a secure, efficient data sharing scheme for dynamic groups in cloud with anonymous authentication of cloud users. By combining group signatures and dynamic broad encryption technique, any cloud user will anonymously share data with other users efficiently. There are some issues regarding storage overhead and encryption computation costs are overcome here.

Keywords— Clouding Computing, Data Sharing, Privacy Preserving, Access Control, Dynamic Groups

I. INTRODUCTION

Basically cloud means data center's hardware and software's. Cloud computing refers to manipulating, configuring and accessing both hardware and software resources from remote location [1].Using cloud computing one can store, share his/ her data to other trusted parties in cloud. To protect data privacy in the cloud, sensitive data, for example, e-mails, personal health records, photo albums, tax documents, financial transactions, and so on, may have to be encrypted by data owners before they are getting to outsourcing to the commercial public cloud [2].By applying cryptography methods for data encryption, keep sensitive data confidential against untrusted cloud server. Further disclosing data decryption keys to authorised users only, but this solution introduce heavy computation overhead on data owner for key distribution. [3] Allowing data owner to depute untrusted cloud server in fine grained access control without disclosing the underlying data contents.

There are some problem related to secure and efficient data sharing for dynamics groups in cloud are as: Now a day's user's identity privacy is major concern. Without guarantee of identity privacy, user may not confident to store data in cloud storage. If we see on other side unconditional users identity privacy leads to snap

up to privacy. Due to this issues traceability allow group manager to show the identity of user when any dispute occurs. Secondly any member in group should capable of data storing and sharing services [3] allow only group manager to store, modify data in the cloud but in multi-owner manner, every user in group can store, share and modify his/ her part of data in entire data file shared by the company. Lastly in any system dynamically user registration and revocation should smoothly occur. In [4], [5], [6] many security scheme are proposed. In their approaches, data owners store his/her data in cloud and distribute corresponding decryption keys to authorised users but these schemes had some drawbacks related to user registration and revocation.

Secure provenance scheme [7] based on bilinear mapping technique to provide trusted evidence data forensics. [8] Proposed cipher text policy attribute based encryption technique allowing any member in group to share data with other members but revocation problem is not solved in above scheme. Fine grained access control achieving through key policy attribute based encryption [7].In this paper we proposed secure, efficient data sharing scheme which allow user to securely share his/her data to other by untrusted cloud server. Our scheme has some advantages includes, it provides dynamic group sharing, user revocation is made easy, computation overhead of encryption does not corresponds to number of revoked users. Any user in group can anonymously share data files to other. But any dispute will occur; data manager can reveal his/her identity by group signature. The remainder of this paper is organized as follows: Section 2 overviews the related work. In Section 3, some elementary terms are reviewed. In Section 4, the proposed scheme is presented in detail, followed by the results in section 6. Finally, we conclude the paper in Section 7

II. RELATED WORK

[1] Defines cloud refers to data centre's hardware and software. They describes obstacles and opportunities in cloud computing. S.Kamara[2] focuses on encrypting sensitive information before it is outsourced to untrusted cloud storage. They also lights on various architecture of cryptographic storage services like a consumer of cryptographic storage architecture, an enterprise architecture.[4] Kallahalla et al. proposed cryptographic cloud storage system that enables secure file sharing on untrusted cloud server and that system named as "Plutus". File get divided into file-groups and encrypting each file group with unique file block key and then data owner can share the file groups with others through lockbox key, this lockbox key generally used for encrypting file-block keys. But it has some drawbacks includes file-block keys need to be updated and distributed again for user revocation.[5] Proposed a security mechanism that improves the security of a network file system without making any changes to the file system or network server. In Sirius, files have two parts: File metadata and file data, stored on untrusted server. The file metadata has the access control information including a series of encrypted key blocks and these key blocks are encrypted under the public key of authorised users. But the size of metadata increased with number of authorised users. [10]("Revocation and tracing") solved the problem of efficient key revocation by NNL construction. But it didn't support for dynamics groups in clouds besides that computation overhead of encryption increases linearly with the sharing scale.

Proxy Re-Encryption [6] allows a proxy to transform a cipher text computed under Alice's public key into one that can be open by Bob's secret key. Using Proxy Re-Encryption scenario data owner encrypts block of content with unique and symmetric keys and further these symmetric content keys are encrypted under a master public key. For providing access control, cloud server uses Proxy Re-Encryption for directly re-encrypt appropriate contents key from master public key to allowing users public key. Due to this method malicious revoked user can read decryption keys of encrypted content blocks. In an ABE[9] system, a user's keys and ciphertexts are labelled with sets of descriptive attributes and a particular key can decrypt a particular ciphertext only if there is a match between the attributes of the ciphertext and the user's key. A secure, scalable and fine-grained data access control scheme [3] is based on the combination of KP-ABE, Proxy Re-Encryption, and Lazy Re-Encryption technique. KP-ABE allows data owner to delegate computation tasks for providing access control to untrusted cloud servers without disclosing actual data contents. Also user secret key updating process delegated to cloud server by group manager. So it is somewhat advantageous regarding computation overhead on server not on client side. But KP-ABE scenario did not provide multiple owner data sharing.

Secure provenance scheme [7] based on bilinear mapping, group signatures and cipher text policy based encryption techniques. The system in their scheme is characterised by providing the information confidentiality on sensitive documents stored in cloud, anonymous authentication on user access and provenance tracking on dispute documents. In provenance technique a data object can report who created and who modified its contents. Therefore, once a dispute rises in a document stored in cloud, provenance is important for data forensics to provide digital evidences for post investigation. User revocation is not suitably implemented in [7]. Short group signature [10] provides anonymity of data owner. The system in their scheme is based on strong Diffie-Hellman assumptions. For privacy preserving in data sharing, group signatures are needed. From the above analysis it is clear that we want a system that provides efficiency, security, access control, user's identity privacy during storing and sharing data by cloud server.

Here we proposed a system that offers features as:

1) ***Data Sharing:*** Any users in group can securely share and store data on untrusted cloud.

2) ***Computation overhead:*** Encryption computation overhead is independent to number of revoked users.

3) ***User revocations:*** user revocation will be done without updating the private keys of the remaining users.

III. ELEMENTARY TERMS

A. Bilinear maps:

Bilinear groups are a set of three abstract algebraic groups, G1, G2 and GT, together with a deterministic function e, called a bilinear map that takes as input one element from G1 and one element from G2 and outputs an element in GT. Two of the main applications of bilinear groups are proxy re-signatures and proxy re-encryption. First we will learn some concept related to bilinear mapping.

1) G1and G2 are two are two cyclic group cyclic groups of prime order p
2) g1 is a generator of G1 and g2 is a generator of G2;
3) ψ is a computable isomorphism from G1 to G2, with $\psi(g2)=g1$ and
4) e is a computable map $e : G1 \times G2 \rightarrow GT$ with the following properties:

Bi-linearity: for all $u \in G_1$, $v \in G_2$ and a, $b \in Z$, $e(u^a, v^b) = e(u, v)^{ab}$.

Non-degeneracy: $e(g_1, g_2) \neq 1$.

Bilinear groups are used to construct short group signatures and the isomorphism ψ is only needed for the proofs of security.

B. Group Signature:

The group signature [11] are "generalization" of credentials/membership authentication scheme in which one person proves that he belong to certain groups. The architecture of a group signature scheme consists of the group manager and multiple group members. Group signature have some properties like only members of the group can sign messages, the receiver can verify that it is a valid group signature but cannot discover group member made it and lastly if necessary, the signature can be "opened", so that the person who signed the message is revealed.

C. Dynamic broadcast encryption:

In broadcast encryption scheme [12] broadcaster (center) broadcasting encrypted data to set of users so that only privileged subset of users will decrypt the data. Dynamic broadcast encryption provides anonymity and traceability.it provides ability to group manager to dynamically include new member. By using this encryption technique new user can decrypt the data stored in the cloud before their participation, and revoked users are unable to decrypt the data moved into the cloud after the revocation. Storing and sharing data with others members in group is done efficiently.

IV. SECURE DATA SHARING SCHEME

Cloud computing provides ability to deliver applications as services over internet and those services provided by data center's hardware and software's like *Saas*, *Iaas*, *Paas* etc. Cloud computing provides economical and efficient solution for sharing group (e.g. Company) resources among multiple cloud users (e.g. Staffs of company). Cloud servers are usually operated by commercial providers which are very likely to be outside of the trusted domain of the users [3]. When a user stores some sensitive information in a cloud, the confidentiality of this sensitive information is of concern to the user [7]. The cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes [13], [14], but will try to learn the content of the stored data and the identities of cloud users. In our system group manger the group manager compute the revocation parameters and make the result public available by migrating them into the cloud. Such a design can significantly reduce the computation overhead of users to encrypt files and the cipher text size.

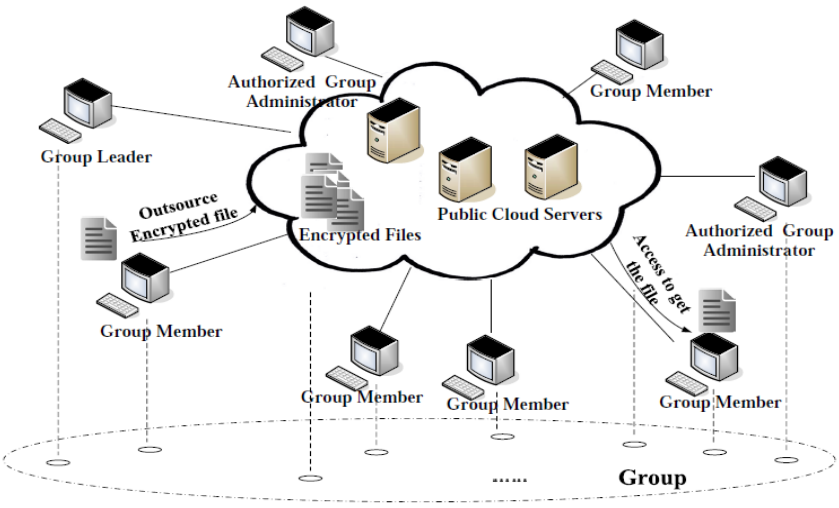

Fig. 1 Dynamic group in cloud

D. Elements of data sharing scheme:

4) Cloud Server: cloud server is data centre's hardware and software's which provides storage, computing services.

5) Group manager: Group manager one who responsible for parameter generation, user registration, users revocations and disclosing real identity of data owner when dispute occurs.

6) Group Members: Group members are group of authorised users that will store their private sensitive data into cloud and share that data with other members in group.

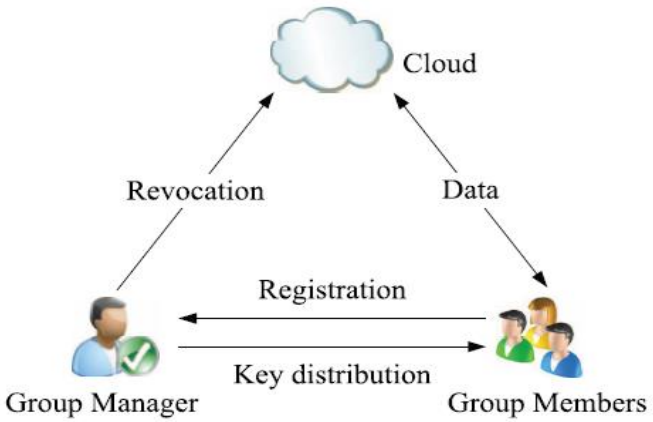

Fig. 2 Architecture of data sharing in cloud group

E. System Modules:

7) Cloud Module:

In this 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. However,

the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. Similar to we assume that the cloud server is honest but curious. That is, the cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes, but will try to learn the content of the stored data and the identities of cloud users.

8) Group Manager Module:

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.

Therefore, we assume that the group manager is fully trusted by the other parties. The Group manager is the admin. The group manager has the logs of each and every process in the cloud. The group manager is responsible for user registration and also user revocation too.

9) Group Member Module:

Group members are a set of registered users that will

1. store their private data into the cloud server and
2. Share them with other users in the group.

Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company. The group member has the ownership of changing the files in the group. Anyone in the group can view the files which are uploaded in their group and also modify it.

10) File Security Module:

1. Encrypting the data file.

2. File stored in the cloud can be deleted by either the group manager or the data owner. (i.e. The member who uploaded the file into the server).

11) 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.

12) 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.

V. RESULTS

Fig. 3 Home Page

Fig. 4 Manager Login Page

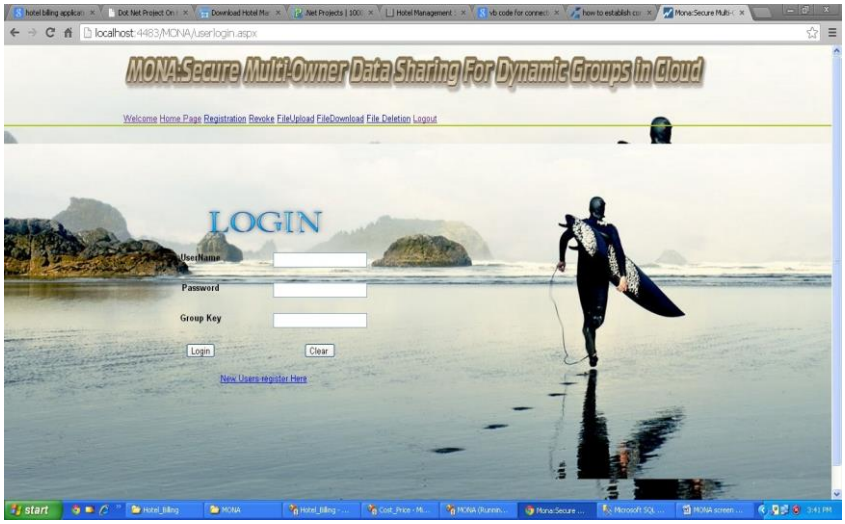

Fig. 5 Member Login Page

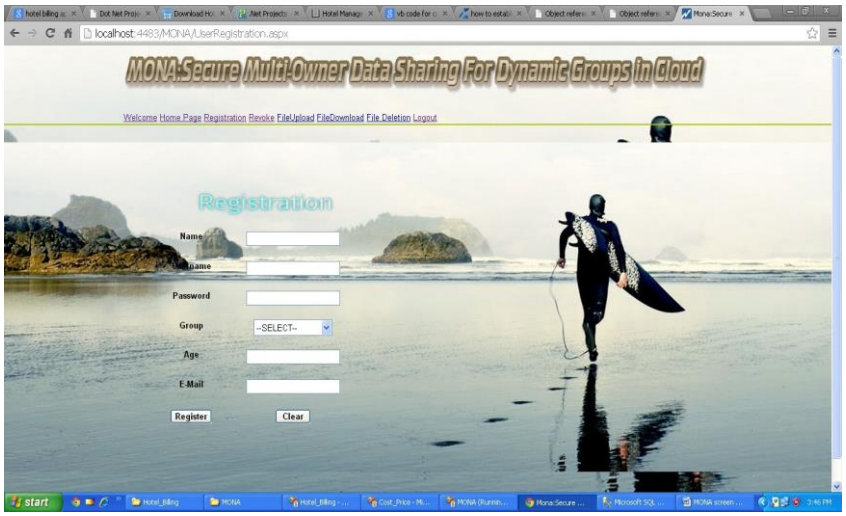

Fig. 6 User Registration Page

Fig. 6 User Revocation Page

VI. CONCLUSION

In this paper, we design secure, efficient multiple owner data sharing scheme for dynamic groups with anonymity of users in untrusted cloud environment. In our scheme member of group can easily share his/ her data to other users efficiently by using group signature and broadcast encryption technique. Identity privacy is archived through anonymity of data owner with bilinear mapping technique. Beside that user revocation is done very smoothly as well as computation overhead is independent on number of revoked 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] 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, "ImprovedProxy 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. Boneh, X. Boyen, and H. Shacham, "Short Group Signature," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-55, 2004.

[11] D. Chaum and E. van Heyst, "Group Signatures," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 257-265, 1991.

[12] A. Fiat and M. Naor, "Broadcast Encryption," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.

[13] B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud," Proc. 10th Int'l Conf. Applied Cryptography and Network Security, pp. 507-525, 2012.

[14] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.

