Secure Multi-owner data Sharing for dynamic group using "MONA" in the Cloud Computing

Miss Tejashri J. Madavi, Dr. S. S. Sherekar, Dr. V. M. Thakare

Abstract— The cloud computing plays a key role for sharing group resource among their users. The aim of the cloud computing is secure data sharing in dynamic cloud computing. It implies that users in the group can securely share data with others by the untrusted cloud. Due to the frequent changes of membership maintaining multi owner data is becoming a complicated task and also sharing of data in an untrusted cloud is also a major challenge. For that reason we introduce the MONA for dynamic groups in the cloud and it supports for group signature and broadcast encryption techniques. Therefore any cloud user can share data with the others. Cloud computing provides an economical and efficient solution for sharing resource among cloud users. This method is able to the support dynamic groups capably; new granted users can directly decrypt data files uploaded before their participation without contacting with data owners.

Index Terms— Cloud Computing, Data Sharing, Dynamic Groups, Privacy Maintenance, Access Control, Security.

1 Introduction

CLOUD computing provide easy-access to computers and their functionality over the Internet or a local area network. Users of a cloud request this accessed from a set of web services that manage a group manger of computing resources. When granted, a fraction of the resources in the group is dedicated to the requesting user until he or she release them. It is called "cloud computing" because the user cannot actually see or specify the physical location and the organization of the equipment hosting the resources they are allowed to use [2]. The resources are drawn from a cloud of resources when they are granted to a user and returned to the cloud when they are released. A "cloud" is a set of machines and web services that apply in cloud computing.

Cloud computing is providing the characteristics such as low maintenance and resource sharing of data. Because of these two characteristics it became a different for the traditional technology. Amazon and such others are providing various services to the cloud users. Cloud providers offering a basic service for the users is data storage [9]. For example the company allows its entire staff to store and share files by using the cloud. By using this staff can get rid of local storage and maintenance but the difficulty raised here is Confidentiality. For this purpose we use the encrypted data files to store in the cloud but still these are some challenging issue. Cloud computing is providing the identity privacy as one of its obstacles without this user may not show interest to use the cloud systems. Here unconditional identity is giving a chance to privacy problems [7]. In single-owner manner only the manager can store, share and modify the files in the cloud where as in multiple-owner any one of the group member can share, store or modify the data so that all the members can enjoy the storing and sharing of data across the cloud. In his it also maintains the revocation list that gives the information about the current group members. Changes of membership make secure data sharing highly difficult key management is also become difficult for every change of membership in the list [8].

1.1 Basic Concept of Mona

Cloud computing is providing the basic characteristics such as low maintenance and resource sharing. Because of these two characteristics it became an alternative for the traditional technology. Amazon and such others are providing various services to the cloud users.

Cloud providers offering a basic service for the users is data storage. In case the company allows its entire staff to store and share files by using the cloud. The staff can get rid of local storage and maintenance but the problem raised here is Confidentiality. For this purpose we use the encrypted data files to store in the cloud but still these are some challenging issue.

Cloud computing is providing the identity privacy as one of its obstacles without this user may not show interest to use the cloud systems .Here unconditional identity is giving a chance to privacy problems. In single-owner manner only the manager can store, share and modify the files in the cloud where as in multiple-owner any one of the group member can share, store or modify the data, so that all the members can enjoy the storing and sharing of data across the cloud.

In his it also maintains the revocation list that gives the information about the current group members. Changes of membership make secure data sharing highly difficultly. Key management is also become difficult for every change of membership in the list. To solve the above challenging issues here we introduced the MONA. This paper mainly includes:

1. Multi-owner data sharing-any one of the group member can securely share and store the data.
2. Dynamic group management-new users can decrypt the data that are uploaded without contacting the data owners.
3. Secure sharing and privacy preserving access control to users is providing. Hence whenever dispute occur the data owners real identities will be revealed by group manager.
4. We also provide strict security analysis.

2 Related Work

Detailed Zhiwei et al. [1] proposed a watermarking method in the architecture of cloud computing, to mitigate the risks of insider disclosures. Private health information once confined

to local medical institutions is migrating onto the Internet as an Electronic Health Record (EHR) that is accessed by cloud computing. The author proposed an insider threat model for the health data storage in the cloud, finding the security gaps. In cloud computing the cloud-based watermarking method including architecture and implementation, for enhancing the cloud security. Rob et al. [2] describe a study in the domain of health informatics which includes some new requirements for patient confidentiality in the context of medical health research. The author present a prototype which takes health records from a commercial data provider, anonymises them in an innovative way and makes them available within a secure cloud-based Virtual Research Environment (VRE). Data anonymity is modified as required for individual researchers' needs and principles committee approval. VREs are with dynamism configured to model each researcher's personal research environment while maintain the data integrity, attribution generation and patient confidentiality. Sven et al. [3] proposed privacy in business processes for providing personalized services is currently a matter of trust. Business processes require the disclosure of personal data to third parties and users are not able to control their usage and so their further disclosure. The current work on usage control mainly considers formalization of usage rules. The author survey on digital watermarking as a way of enforce obligation for further revelation of personal data without fixed trust in service providers. Yuyu et al. [4] proposed new SaaS Confidentiality Risk Management Framework based on literature research, expert talks and the working experience. It enhances the client side confidentiality management in a public SaaS included IT environment and especially focuses on small to medium sized enterprises, which are often meet with rigid contracts enforced by cloud service providers and have weak and lacking ability to consult Service Level Agreements (SLAs). Tatiana et al. [5] proposed EHR as a subset of electronic medical record shared across health centre (HC) by medical workers. The cloud computing approach does not just provide sufficient data storage capacities and facilitate storing of health data in one central place.

3 Analysis of Existing System

To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. The designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task.

In the existing System data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users [11]. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys. However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively [12].

In the existing Systems, identity privacy is one of the most significant obstacle for the wide deployment of cloud computing. Without the security of identity privacy, users may be unwilling to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers. On the other hand, unconditional identity privacy may incur the abuse of privacy [13]. For example, a misbehave staff can deceive others in the company by sharing false files without being traceable. Only the group manager can store and modify data in the cloud. The changes of membership make secure data sharing extremely difficult the issue of user revocation is not addressed. But the disadvantage is user revocation is not supported. Compared with the above solutions MONA offers some unique features such as

1. Any one of the group member can store and share data files in the cloud.
2. The complexity of encryption and size f cipher texts are independent.
3. Revocation list is available without updating the keys.
4. New user can directly decrypt the files stored in the cloud without his participation.

4 Proposed System

We proposed a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the untrusted cloud. Our proposed scheme is able to support dynamic groups efficiently. The new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users. We provide secure and privacy-preserving access control to users, which guarantee any member in a group to anonymously utilize the cloud resource. The real identities of data owners can be revealed by the group manager when dispute occur. We provide accurate security analysis, and perform extensive simulations to show the efficiency of our scheme in terms of storage and computation overhead.

The following figure shows the cloud computing architecture with the example. Here we are using an organization who are using the cloud to enable its staff members to share data files in the same department or in group. It mainly consists of three major things. Those are Group Manager in our example he is Organization manager), Group members (Users/Staff of the Organization), and the third one is the important one cloud. Cloud is operated by the CSPs and provides price abundant storage services.

But the cloud is not fully trusted because it is outside of the user's trusted domain. Group manager take care of parameters generation, user registration, user revocation and tracing real identity of a dispute data owner. Group members are registered users who can share their private data in the cloud with their group members. Here group members keep on changing that is due to staff resignation and new employee joining. The major design goals of this project are access control, data confidentiality, anonymity, traceability and efficiency.

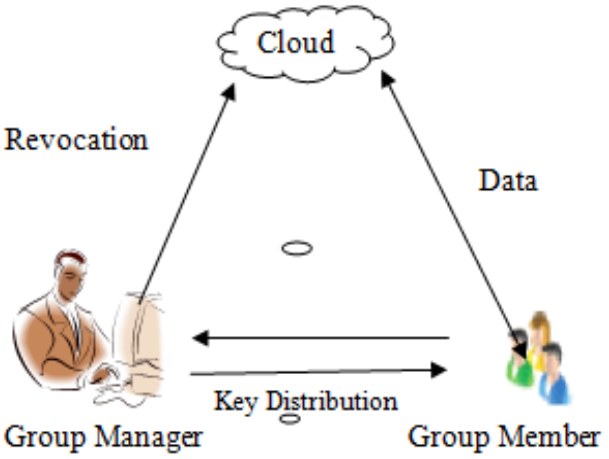

Fig. 1. Proposed System Model.

5 Expected Results and Analysis

If The experiments are performing on Windows 7 with 64 bit processor. The proposed prototype system is implementing in Asp.net Microsoft Visual Studio 12. In this AES-256 implementation is used for encryptions & back end perform on Microsoft SQL Management studio-2008. For achieving the secure data sharing for dynamic groups in the cloud here we combine group signature technique and dynamic broadcast encryption technique. Particularly the group signature enables users to anonymously use the cloud resources, and the dynamic broadcast encryption technique allows data owners to securely share their data files with others even with the new users. Here tackling the user revocation is done by the group manager and the group manager provides the revocation list in the public by migrating them into the cloud. It reduces the computation overhead. In MONA the computation cost and the cipher text size are constant and those are independent of revoked users.

The modules of the system are shows below:

1. *Registration:* In this module a User has to register first, and then only he/she has to access the data base.
2. *Login:* In this module, any of the above mentioned user has to login, they should login by giving their email and password key.
3. *Fileupload:*
   In this module Manager (Owner) uploads the file (along with meta data) into database, with the help of this metadata and its contents, the end user has to download the file. The uploaded file was in encrypted form, only registered user can decrypt it. Even CSP can only view the encrypted file form.
4. *Chart Creation:* User can view the chart, which is dynamically created by calculating the size of the file.
5. *File Download:* The Registered users can download the file and can do updates. The modified file will be uploaded into cloud server by the user.
6. *User Deletion:* Manager (admin) can reject the user, so as that rejected user doesn't login and access the database.

6 Advantages of Proposed System

1. Any user in the group can store and share data files with others by the cloud.
2. The encryption complexity and size of cipher texts are independent with the number of revoked users in the system.
3. User revocation can be achieved without updating the private keys of the remaining users.
4. A new user can directly decrypt the files stored in the cloud before his participation.

7 Conclusion

In this paper, we design a secure data sharing scheme, Mona, for dynamic groups in an untrusted cloud.The user is able to share the data in the cloud with their group without edifying their identities. The MONA supports for efficient user revocation and it can be achieved by public revocation list. The updating of the others private keys is not needed for MONA. The storage overhead and computation costs are constant. If the group manager fails to handle the files, the reliability and scalability problems arise. In future for solving the reliability and scalability issues we further introduce the back-up group manager. In case of any failures of group manager the backup group manager handles those trouble hence the reliability and scalability increases.

Acknowledgment

At the outset, I would like to thank my guide, Dr. S. S. Sherekar, Department of Computer Science & Engg, SGB Amravati University, Amravati. I would like to give special thanks to our Research Center Head Dr. V. M. Thakare, PG Department of Computer & Engg, SGB Amravati University. I would like

to mention the special thanks to AICTE for providing the funds under RPS, under which I am able to carry out my research work.

REFERENCES

[1] *Zhiwei Yu, Clark Thomborson, Chaokun Wang, Jianmin Wang and Rui Li."A Cloud-Based Watermarking Method for Health Data Security", IEEE paper 2012 ISBN: 978-1-4673-2362-8/12.*

[2] *Rob Smith, Jie Xu, Saman Hima & Dr. Owen Johnson."GATEway to the Cloud", IEEE Computer Society 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering, DOI 10.1109/SOSE.2013,46.*

[3] *Sven Wohlgemuth, Isao Echizen and Noboru Sonehara."On Privacy-Compliant Dislosure of Personal Data to Third Parties using Digital Watermarking", Journal of International Hiding and Multimedia Signal Processing VOL 2, NO. 3, pp 2073-4212, July 2011.*

[4] *Yuyu Chou, Olga Levina, Jan Oetting."Enforcing Confidentiality in a SaaS Cloud Environment", IEEE paper 2011 19th Telecommunications forum TELFOR, ISBN: 978-1-4577-1500-6/11.*

[5] *Tatiana Ermakova and Benjamin Fabian."Secret Sharing for Health Data in Multi-Provider Clouds", IEEE Computer Society 2013 IEEE International Conference on Business Informatics, DOI 10.1109/CBI.2013.22.*

[6] *M. Armbrust, A. Fox, R. Griffith, "A View of Cloud Computing", Comm. ACM, Vol. 53, No. 4, pp. 50-58, Apr. 2010.*

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

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

[9] *M.Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, K. Fu,"Plutus: Scalable Secure File Sharing on Untrusted Storage", Proc.USENIX Conf. File and Storage Technologies, pp. 29-42, 013.*

[10] *E. Goh, H. Shacham, N. Modadugu, D. Boneh, "Sirius: Securing Remote Untrusted Storage", Proc.Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2013.*

[11] *G.Ateniese, K. Fu, M. Green, S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage", Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2012.*

[12] *R. Lu, X. Lin, X. Liang, 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, 2011.*

[13] *V. Goyal, O. Pandey, A. Sahai, B. Waters,"Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2011.*

[14] *D. Naor, M. Naor, J.B. Lotspiech,"Revocation and Tracing schemes for Stateless Receivers", Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2013.*

[15] *S. Ruj, A. Nayak, and I. Stojmenovic, "Dacc: Distributed access control in clouds," in 10th IEEE TrustCom, 2011.*