Security Enhancement for Sharing Data within Group Members in Cloud

Sachin Ghode[1], Prof. Dr. Sachin Bojewar[2]

[1]M.E. Student, Department of Information Technology, VIT, Wadala, Mumbai, India
[2]Assistant Professor Department of Information Technology, VIT, Wadala, Mumbai India

***Abstract**: Cloud computing provide a secure way for data sharing and maintaining its security by preventing collusion attack in cloud. Due to the incessant change of the enrollment, protecting the sharing information is a challenging task, particularly for an untrusted cloud because of the conspiracy assault. In this paper, we propose a safe information sharing plan for element individuals. To*

begin with, client in the data sharing system upload their file with the encryption using private key. This property is especially important to any large scale data sharing system, as any user leak the key information then it will become difficult for the data owner to maintain security of the information. In this paper provide a concrete and efficient instantiation of scheme, prove its security and provide an implementation to show its practicality. There are lots of challenges for data owner to share their data on servers or cloud. There are different solutions to solve these problems. These techniques are very much critical to handle key shared by the data owner. This paper will introduce the trusted authority to authenticate user those who have the access to the data on cloud. The trusted authority module receives encrypted file using AES Algorithm from the data owner. It stores key in its database which will be used during the dynamic operations and to determine the cheating party in the system (CSP or Owner). Trusted authority send file to CSP module to store on cloud.

1. Introduction

As cloud computing becomes prevalent, more and more sensitive information By storing their data into the cloud, the data owners can be relieved from the burden of data storage and maintenance, so as to enjoy the on-demand high quality data storage service cloud server are not in the same trusted domain may put the outsourced data at risk.

In this work, a secure data sharing scheme, which can achieve secure key distribution and data sharing for a dynamic group in the cloud. The main contributions of this scheme include:

- A secure data sharing scheme can be protected from collusion attack. The revoked users cannot be able to get original data files once they are revoked even if they conspire with the untrusted cloud. This scheme can achieve secure user revocation with the help of polynomial function.

- This scheme can achieve fine-grained access control. With the help of the group user list, any user in the group can use the source in the cloud and revoked users cannot access the cloud again [1].

- A way for key distribution without any secure communication channels. The users secure can securely obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user.

A key challenge in moving to the cloud is to ensure and build confidence that user data is handled securely in the cloud. A recent Microsoft survey found that 58 percent of the public and 86 percent of business leaders are excited about the possibilities of cloud computing. But, more than 90 percent of them are worried about security, availability, and privacy of their data as it rests in the cloud [2]. There is tension between user data protection and rich computation in the cloud. Users want to maintain control of their data, but also want to benefit from rich services provided by application developers using that data. Cloud computing have aimed to allow access large amounts of data in a fully virtualized manner. Cloud computing allows for the sharing and scalable deployment of services from almost any location, for which the customer can be charged based on actual usage. Security is needed against unauthorized access and to reduce risks of data stealing. The main aim of security is to provide availability, confidentiality, integrity to the data [3]. There are so many risk associated with the cloud network like data can be hacked by an unauthorized person. Data can be changed by third party while transferring the data. Thus to provide security to cloud data we proposed a system which can achieve secure key distribution and data sharing for dynamic group.

2. Related Work

Following are some existing method of cloud storage:

A. Cryptographic Cloud Storage:

Many researchers have proposed stored encrypted data in the cloud to define against CSP. S. Kamara and K. Lauter [4] in their work “Cryptographic cloud storage” considered the problem of building a secure cloud storage service on top of a public cloud infrastructure where the service provider is not completely trusted by the customer. Its core, the architecture consists of three components: a data processor (DP), that processes data before it is sent to the cloud; a data verifier (DV), that checks whether the data in the cloud has been tampered with; and a token generator (TG), Under this approach, users are revoked by having a third party to re encrypt data such that previous keys can no longer decrypt any data.

B. Plutus: Scalable Secure File Sharing On Untrusted Storage:

Which uses a lockbox to protect only the keys. Mechanisms that Plutus uses to provide basic file system security features-(1) To detect and prevent unauthorized data modifications, (2) To differentiate between read and write access to files, and (3) To change users access privileges. In encrypt-on-disk file systems, the clients encrypt all directories and their contents. Which used a single key to encrypt an entire directory of files. R. Lu [5] in their work

“Plutus: Scalable secure file sharing on untrusted storage” introduces a new secure file system which strives to provide strong security even with an untrusted server. The main feature of Plutus is that all data is stored encrypted and all key distribution is handled in a decentralized manner. All cryptographic and key management operations are performed by the clients, and the server incurs very little cryptographic overhead.

C. Mona: Secure Multi-Owner Data Sharing For Dynamic Groups In The Cloud:

With the character of low maintenance, cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent change of the membership. In this paper, we propose a secure multi owner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. In addition, we analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments[6]. Kallahalla et al [7] presented a cryptographic storage system that enables secure data sharing on untrustworthy servers based on the techniques that dividing files into file groups and encrypting each file group with a file-block key. Yu et al exploited and combined techniques of key policy attribute based encryption, proxy re-encryption and lazy re-encryption to achieve fine-grained data access control without disclosing data contents.

3. Proposed Work

In this paper, we propose a protected information sharing plan, which can accomplish secure key distribution and information sharing for element bunch. The primary commitments of our plan include:

We give a safe approach to key distribution without any safe correspondence channels. The clients can safely get their private keys from gathering administrator with no Certificate Powers due to the confirmation for people in general key of the client. Our plan can accomplish fine-grained access control, with the assistance of the gathering client list, any client in the gathering can utilize the source in the cloud and revoked clients can't get to the cloud again after they are revoked.

We propose a protected information sharing plan which can be shielded from intrigue assault. The revoked clients cannot have the capacity to get the first information documents once they are repudiated regardless of the fact that they plot with the untrusted cloud. Our plan can accomplish secure client repudiation with the assistance of polynomial capacity.

Our plan can bolster dynamic gatherings productively, when another client joins in the gathering or a client is denied from the gathering, the private keys of alternate clients don't should be recomputed and overhauled. We give security investigation to demonstrate the security of our plan. Furthermore, we additionally perform reproductions to exhibit the productivity of our plan. We give security investigation to demonstrate the security of our plan. Furthermore, we additionally perform reproductions to exhibit the productivity of our plan.

Cloud Server:

The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them.

Data Owner: (Group Member)

In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the data file and then store in the cloud. The Data owner can have capable of manipulating the encrypted data file. And the data owner can set the access privilege to the encrypted data file.

Group Manager:

The Group Manager who is trusted to store verification parameters and offer public query services for these parameters. In our system the Trusted Third Party, view the user data and uploaded to the distributed cloud. In distributed cloud environment each cloud has user data. The Group Manager will perform the revocation and un revocation of the remote user if he is the attacker or malicious user over the cloud data.

Data Integrity:

Data Integrity is very important in database operations in particular and Data warehousing and Business intelligence in general. Because Data Integrity ensured that data is of high quality, correct, consistent and accessible.

Data Consumer: (End User / Group Member)

In this module, the user can only access the data file with the encrypted key if the user has the privilege to access the file [9]. For the user level, all the privileges are given by the GM authority and the Data users are controlled by the GM Authority only. Users may try to access data files either within or outside the scope of their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges.

System Architecture:

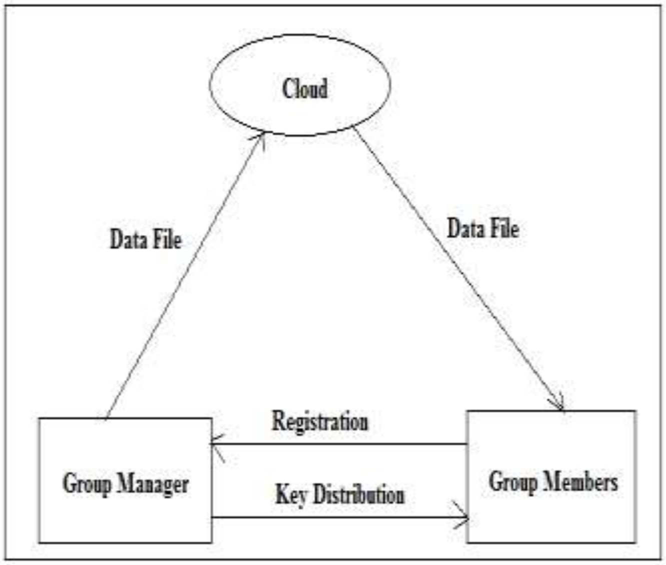

Figure 1. System Architecture

As illustrated in the above figure, the system model consists of three different entities: the cloud, a group manager and a large number of group members. The cloud, maintained by the cloud service providers, provides storage space for hosting data files in a pay-as you-go manner. However, the cloud is untrusted since the cloud service providers are easily to become un-trusted. Therefore, the cloud will try to learn the content of the stored data.

Group manager takes charge of system parameters generation, user registration, and user revocation. In the practical applications, the group manager usually is the leader of the group. Therefore, we assume that the group manager is fully trusted by the other practices.

Group members (users) are a set of registered users that will store their own data into the cloud and share them with others. In the scheme, the group membership is dynamically changed, due to the new user registration and user revocation

4. Conclusion

This scheme designs a secure anti-collusion data sharing scheme for dynamic groups in the cloud. In this scheme, the users can securely obtain their private keys from group manager without any Certificate Authorities and secure communication channels. Also, this scheme is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated. Moreover, this scheme can achieve secure user revocation, the revoked users can not be able to get the original data files once they are revoked even if they conspire with the untrusted cloud.

5. Acknowledgement

I express my sincere thanks to my project guide Prof. Dr. Sachin Bojewar who always being with presence & constant, constructive criticism to made this paper. I would also like to thank all the staff of Information Technology department for their valuable guidance, suggestion and support through the project work, who has given co-operation for the project with personal attention. Above all I express our deepest gratitude to all of them for their kind-hearted support which helped us a lot during project work. At the last I thankful to my friends, colleagues for the inspirational help provided to me through a project work.

6. REFERENCES

[1] Data Sharing Scheme for Dynamic Groups in the Cloud", IEEE Transactions on Parallel and Distributed Systems, 2015.

[2] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proc. Netw. Distrib. Syst. Security Symp. 2003, pp. 131–145.

[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] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc.Int. Conf. Financial Cryptography Data Security, Jan. 2010, pp. 136–149.

[5] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure provenance: The essential of bread and butter of data forensics in cloud computing," in Proc. ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282–292.

[6] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Int.Conf. Practice Theory Public Key Cryptography Conf. Public Key Cryptography, 2008, pp. 53–70.

[7] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in Proc. USENIX Conf. File Storage Technol., 2003, pp. 29–42.

[8] 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.

[9] M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy based content sharing in public clouds," IEEE Trans. Know. Data Eng., vol. 25, no. 11, pp. 2602– 2614, Nov. 2013.