ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Data Access Control Scheme with Prevention of Collusion Attack in Cloud Environment

Jyoti Pingat[1], Prof. P. R. Ugale[2]

M.E. Student, Department of Computer Engineering, SPCOE, Otur, India[1]

Assistant Professor, Department of Computer Engineering, SPCOE, Otur, India[2]

ABSTRACT: Due to the incessant change of the participation, sharing data while giving security saving is as yet a complicated issue, particularly for an untrusted cloud because of the collusion attack. In addition, for existing plans, the security of key transfer depends on the protected correspondence channel, not withstanding, to have such channel is a solid presumption and is troublesome for practice. In this paper, we propose a protected data sharing plan for dynamic individuals. To start with, we propose a safe path for key appropriation with no safe correspondence channels, and the clients can safely acquire their private keys from gathering director. Second, our plan can accomplish fine-grained get to control, 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. Third, we can ensure the plan from collusion attack, which implies that revoked clients can't get the first data record regardless of the possibility that they plan with the untrusted cloud. At long last, our plan can accomplish fine effectiveness, which implies past clients require not to refresh their private keys for the circumstance either another client participates in the gathering or a client is revoked from the gathering.

KEYWORDS: Sharing Data; Data Sharing; Collusion Attack; Key Transfer

I. INTRODUCTION

Cloud Computing, have the characteristics of natural information sharing and low support, gives a tremendous use of resources. In Cloud Computing, cloud administration suppliers provide a reflection of boundless storage room for customers in order to host the information. It provide some support for customers, with reducing their money related overhead of information administrations by moving the nearby administrations framework into cloud servers.
In cloud computing, cloud service providers offer an abstraction of infinite storage space for clients to host data. It can help clients reduce their financial overhead of data managements by migrating the local managements system into cloud servers. However, security concerns become the main constraint as we now outsource the storage of data, which is possibly sensitive, to cloud providers. To preserve data privacy, a common approach is to encrypt data files before the clients upload the encrypted data into the cloud. Unfortunately, it is difficult to design a secure and efficient data sharing scheme, especially for dynamic groups in the cloud. 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. However, the file-block keys need to be updated and distributed for a user revocation; therefore, the system had a heavy key distribution overhead. However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the revoked users.
The 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. However, the single-owner manner may hinder the implementation of applications, where any member in the group can use the cloud service to store and share data files with others. However, the scheme will easily suffer from the collusion attack by the revoked user and the cloud. The revoked user can use his private key to decrypt the encrypted data file and get the secret data after his revocation by conspiring with the cloud. In the phase of file access, first of all, the revoked user sends his request to the cloud, and then the cloud responds the corresponding encrypted data file and revocation list to the revoked user without verifications. Next, the revoked user can compute the decryption key with the help of the attack algorithm. Finally, this attack can lead to the revoked users getting the sharing data and disclosing other secrets of legitimate members. Unfortunately, the secure way for sharing the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

personal permanent portable secret between the user and the server is not supported and the private key will be disclosed once the personal permanent portable secret is obtained by the attackers.

II. BACKGROUND

The environment of cloud computing consist of five qualities, three conveyance models and four organization models. The five vital qualities of cloud computing are including first stratum are: area free asset pooling that is supplier assets pooled to server various customers, on-interest self-administration, fast flexibility which is capacity to rapidly scale in/out administration, expansive system get to, and measured administration that is leasing the administrations use per pay premise.

1. Private cloud. The cloud infrastructure is operated single for one organization. It may be managed by the organization or a third party and may exist on premise or off premise. Arguably this may be the most secure type of infrastructure, depending on the nature of the controls deployed and the diligence of the operator.

2. Community cloud. In this model, several organizations shared the cloud infrastructure and supports a specific community or interest group that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

3. Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

4. Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).
Three Cloud Conveyance models are Iaas, PaaS and SaaS includes center stratum of cloud computing environment.
In Software as a Service (SaaS), applications are there that are empowered for the cloud. It underpins a design that can run various occasions of it-self which are area . This is only a month to month membership based estimating model and it is stateless. Examples of SaaS are MobileMe, Google docs, Zoho.

In Platform as Services, it incorporates stage on which engineers can compose their applications to be keep running on cloud environment. This stage typically has numerous application administrations accessible for speedy organization. Case of PaaS is Google Application Motor, Microsoft Sky blue, Force.com.

Infrastructure as a Service (IaaS) used by consumer by providing storage, processing, networking, and other fundamental computing resources where the consumer is able to deploy and run software, which can include operating systems and applications. It is highly scaled redundant and shared computing Infrastructure approachable using internet technologies. Examples of this type of delivery model include Amazon EC2, Sun's cloud services, Terremark cloud offering etc.

III. RELATED WORK

Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud: With cloud data services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users. Unfortunately, the integrity of cloud data is subject to skepticism due to the existence of hardware/software failures and human errors. Several mechanisms have been designed to allow both data owners and public verifiers to efficiently audit cloud data integrity without retrieving the entire data from the cloud server. However, public auditing on the integrity of shared data with these existing mechanisms will inevitably reveal confidential information-identity privacy-to public verifiers. In this paper, we propose a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

In particular, we exploit ring signatures to compute verification metadata needed to audit the correctness of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private from public verifiers, who are able to efficiently verify shared data integrity without retrieving the entire file. In addition, our mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one. Our experimental results demonstrate the effectiveness and efficiency of our mechanism when auditing shared data integrity.

Security Challenges for the Public Cloud: In this talk, I will first discuss a number of pressing security challenges in Cloud Computing, including data service outsourcing security and secure computation outsourcing. Then, I will focus on data storage security in Cloud Computing. As one of the primitive services, cloud storage allows data owners to outsource their data to cloud for its appealing benefits. However, the fact that owners no longer have physical possession of the outsourced data raises big security concerns on the storage correctness. Hence, enabling secure storage auditing in the cloud environment with new approaches becomes imperative and challenging.

Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing: Cloud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public audit ability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed.
To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, we utilize and uniquely combine the public key based homomorphism authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.

Computing Encrypted Cloud Data Efficiently under Multiple Keys: The emergence of cloud computing brings users abundant opportunities to utilize the power of cloud to perform computation on data contributed by multiple users. These cloud data should be encrypted under multiple keys due to privacy concerns. However, existing secure computation techniques are either limited to single key or still far from practical. In this paper, we design two efficient schemes for secure outsourced computation over cloud data encrypted under multiple keys. Our schemes employ two non-colluding cloud servers to jointly compute polynomial functions over multiple users' encrypted cloud data without learning the inputs, intermediate or final results, and require only minimal interactions between the two cloud servers but not the users. We demonstrate our schemes efficiency experimentally via applications in machine learning. Our schemes are also applicable to privacy-preserving data aggregation such as in smart metering.

IV. MOTIVATION

Cloud computing, users can achieve an effective and economical approach for data sharing among group members in the cloud with the characters of low maintenance and little management cost. Meanwhile, we must provide security guarantees for the sharing data files since they are outsourced. Unfortunately, because of the frequent change of the membership, sharing data while providing privacy-preserving is still a challenging issue, especially for an untrusted cloud due to the collusion attack. Moreover, for existing schemes, the security of key distribution is based on the secure communication channel, however, to have such channel is a strong assumption and is difficult for practice.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

In this paper, we propose a secure data sharing scheme for dynamic members. Firstly, we propose a secure way for key distribution without any secure communication channels, and the users can securely obtain their private keys from group manager. Secondly, our scheme can achieve fine-grained access control, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked. Thirdly, we can protect the scheme from collusion attack, which means that revoked users cannot get the original data file even if they conspire with the untrusted cloud. In our approach, by leveraging polynomial function, we can achieve a secure user revocation scheme. Finally, our scheme can achieve fine efficiency, which means previous users need not to update their private keys for the situation either a new user joins in the group or a user is revoked from the group. our 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, our 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.

V. SYSTEM ARCHITECTURE

Proposed a scheme that provides a secure way for key distribution without secure communication channels. In which the user can securely obtain their private keys from the group manager without any certificate authority due to the verification for the public key of user. This scheme can achieve fine grained access control. This scheme uses the polynomial function for user revocation so it protect form collusion attack. This scheme support dynamic group efficiency in which private key will not be recomputed and update at the new user joining or user revocation.
.

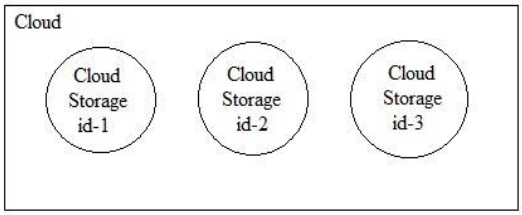

Fig. 1. Cloud Server Storage

In this paper we proposed a scheme that provides the anti-collusion data sharing in multiuser cloud. Firstly the user registration user can register in the system in which user provides the information about him and complete the registration process system provides the user id and password to access the cloud. This information should be managed by the group manager. The uploading user uploads a data into the cloud. The data must be stored in the no. of server in the cloud and the up loader user use the block for the data storage. The block that means the one file must stored in to the no. of blocks in the same server. All the activity should be manage by group manager. The file should be stored as no. of blocks in the server. The two types of encryption algorithm is used for the encryption. The encrypted data stored in server.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

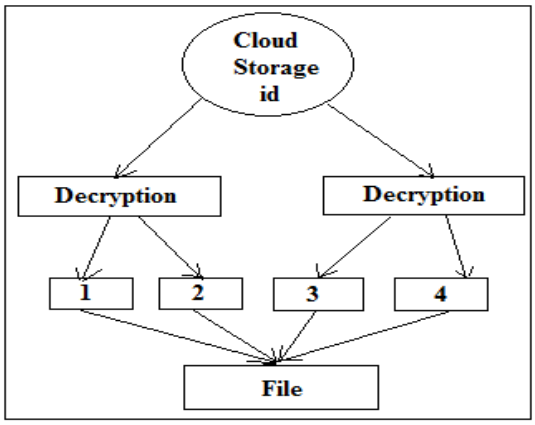

Fig. 2. File Uploading

The downloading user accesses the uploading data. It sends request to the uploading user the uploading user check that request and forwards the data to the requested user id. The uploading user forward the data that contend the information about the file name, stored server id, and no. of blocks used to store that file. The downloader user search that file in the server by its file name. The server request the block no and server id to the downloader, the downloader enter the server id and block no the server granting the access permission of that file to the user. The group manager can manage the information about the group manager and information details about the user it can monitor the activity of the uploading and downloading user. It can maintain the revoked user list if the user must be revoked the manager pleased this user as revoked.

VI. SYSTEM SPECIFICATION AND REQUIREMENTS

A. Hardware Requirements:

- Processor - Pentium -IV
- Speed - 1.1 GHz
- RAM - 256 MB(min)
- Hard Disk - 20 GB

B. Software Requirements:

- Operating System: Windows95/98/2000/XP/7.
- Application Server: Tomcat6.0/7.X.

Front End: HTML, Java, JSP.
Scripts: JavaScript.

- Server side Script: Java Server Pages.

Database: MYSQL 5.0.

- Database Connectivity: JDBC.

VII. PROPOSED ALGORITHM

We propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic group. The below steps are included in this algorithms,

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

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

2. Our 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 after they are revoked.

3. We propose a secure data sharing scheme which can be protected from collusion attack. 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. Our scheme can achieve secure user revocation with the help of polynomial function.

4. Our 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. 5. We provide security analysis to prove the security of our scheme. In addition, we also perform simulations to demonstrate the efficiency of our scheme.

VIII. CONCLUSION

In this paper, we design anti-collusion data sharing scheme for dynamic group in the cloud. In our scheme we use two types of algorithms to encrypt and decrypt the data stored in the cloud for more security that is used to make more difficult system for attack. In this scheme we use forwarding mechanism in which uploading user has authority to forward his data to the other user and requested user I. e downloading user will request for data to the uploading user. All the activity can be manage by the manager.

IX. FUTURE ENHANCEMENT

In this research work, we have reviewed literature on ways to provide a secure environment where a data owner can share data with members of his group while preventing any outsiders from gaining any data access in case of carry out malicious activities on the data owner's data.
Auditing and Accountability in the Cloud is a potential for future research in the context of data sharing in the Cloud. Many users in particular organizations and enterprises gain the benefit from data sharing in the Cloud. However, there is always a likely chance that members of the group can carry out illegal operations on the data such as making illegal copies and distributing copies to friends, general public, etc in order to profit. A future research direction would be to find ways for a data owner to hold accountable any member that carries out malicious activities on their data.

REFERENCES

[1]. S. Kamara and K. Lauter, "Cryptographic Cloud Storage," *in Proc. of FC, January* 2010, pp. 136-149.
[2]. 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.
[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]. Shucheng Yu, Cong Wang, Kui Ren, and Weijing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," *Proc. ACM Symp. Information, Computer and Comm. Security*, pp. 282-292, 2010.
[5]. 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
[6]. 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.
[7]. I.Varun and Vamsee Mohan.B," An Efficient Secure Multi Owner Data Sharing for Dynamic Groups in Cloud Computing", *International Journal of Computer Science and Mobile Computing*, Vol.3 Issue.6, June- 2014, pg. 730-734
[8]. Lan Zhou, Vijay Varadharajan, and Michael Hitchens, "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 12, pp. 1947-1960, December 2013.
[9]. Xukai Zou, Yuan-shun Dai, and Elisa Bertino, "A practical and flexible key management mechanism for trusted collaborative computing," *INFOCOM* 2008, pp. 1211-1219.
[10]. Zhongma Zhu and Rui Jiang," A Secure Anti- Collusion Data Sharing Scheme for Dynamic Groups in the Cloud", *IEEE Transactions on Parallel and Distributed Systems* DOI:10.1109/TPDS.2015.2388446.