A SELF SECURE ANTI COLLUSION DATA SHARING SCHEME FOR DYNAMIC GROUP IN THE CLOUD

V.Punitha[1], Miss.R.Radhika[2]
[1]PG student, Department of Computer Science,
[2]Assistant Professor. Sri Ramanujar Engineering College,Tamil Nadu,India

Abstract: Benefited from 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. In this paper, we propose a secure data sharing scheme for dynamic members. First, 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. Second, 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. Third, 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.

Keywords: Cloud Computing, Security, Private keys,fine grained access control.

I. INTRODUCTION

Cloud computing, with the characteristics of intrinsic data sharing and low maintenance, provides a better utilization of resources. 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 computing. 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. However, the file-block keys need to be updated and distributed for a user revocation, therefore, the system had a heavy key distribution overhead. Other schemes for data sharing on untrusted servers have been proposed. However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the revoked users.

II. PROJECT DEFINITION

Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of the stored data. To maintain the availability of data confidentiality for dynamic groups is still an important and challenging issue. Specifically, revoked users are unable to decrypt the stored data file after the revocation.

III. OBJECTIVE

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. In this paper, we propose a secure data sharing scheme for dynamic members. First, 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. Second, 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. Third, 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.

IV. FEATURES

Advance Encryption Standard (AES)

AES is a symmetric block cipher, this key is expanded into individual sub keys, for each operation round. This process is called key expansion. Its a symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret-key.

ADVANTAGES

Secure protocol for anti-collusion attack.

Faster recovery and processing of data.

This would significantly decrease the processing time of load balancer.

Effective and Efficient usage of cloud Storage Space

DISADVANTAGES

The complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the revoked users.

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.

V. LITERATURE REVIEW

5.1 DATA STORAGE SECURITY IN CLOUD COMPUTING

OBSERVATION

Cong Wang, Qian Wang, and KuiRen AND Wenjing Lou Ensuring Data Storage Security in Cloud Computing, where users can remotely store their data into the cloud so as to enjoy the on demand high quality application and services from a shared pool of configurable computing resources by data out sourcing, uses can be relieved from the burden of local data storage and maintenance. However, the fact that uses 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.

COMMENTS

This paper focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users‟ data in the cloud, authors propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasurecoded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server(s).

5.2 SECURITY CHALLENGES FOR THE PUBLIC CLOUD OBSERVATION

A. Juels and J. Burton S. Kaliski, “PORs: Proofs of Retrievability for Larg Files, ” Proc. of CCS ’07, pp. 584-597, 2007.In this talk, I will 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.

COMMENTS

This paper described a formal “proof of retrievability” (POR) model for ensuring the remote data integrity. Their scheme combines spot-checking and error-correcting code to ensure both possession and retrievability of files on archive service systems

5.3 PRIVACY PRESERVING PUBLIC AUDITING FOR SHARED DATA IN THE CLOUD

OBSERVATION

G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, “Scalable and Efficient Provable Data Possession, ” Proc. of SecureComm ’08, pp. 1-10, 2008.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 to existence of hardware/software failures and human errors. Several machanism 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 thispaper, we propose a novel privacy preserving mechanism that supports public auditing on shared data stored in the cloud.

COMMENTS

This paper described a PDP scheme that uses only symmetric key cryptography. This method has lower-overhead than their previous scheme and allows for block updates, deletions and appends to the stored file, which has also been supported in our work

VI. SYSTEMM ANALYSIS

REQUIREMENT ANALYSIS

6.1 Hardware Requirements

System	: Pentium IV 2.4 GHz.
Hard Disk	: 40 GB.
Floppy Drive	: 1.44 Mb.
Monitor	: 15 VGA Color.
Mouse	: Logitech.
Ram	: 512 MB.

6.2 Software Requirements

Operating system	: Windows 7 Professional.
Coding Language	: Java, Servlet.
Front End Tool	: Net beans 7.0
Database	: MS Sql.
Back End Tool	: SQL Yog.
Load balancer	: Appache
Virtual Machine.	: Tomcat Server

VII. EXISITING SYSTEM

In existence private key distribution is based on the secure communication channel, In this case, which user have private key can share data unfortunately revoked user also can share data. Revoked user means who have changed their membership.

Therefore, secure communication channel is a strong assumption but difficult to use.

Cloud storage is not efficiently utilized. Replica of data is possible.

VIII. PROPOSED SYSTEM

The users can securely obtain their private keys from group manager.

User send request to group manager for access the wanted group, at that time our system provide individual secure key to user without activation.

Then group manager see the requests and activate the keys after confirm them.

After user's private key gets activation, then only user can access the group.

Our scheme have 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.

In our proposed system the group manager performs the below tasks when an new user joins the group or a user has left the particular group,

Update the whole user name list.

Generate a secure key and encrypt the key without activation and send to the updated user list.

Update the rights in the cloud server.

We proposed public cloud named Dropbox for data storage.

Group manager makes sure that the revoked users cannot access the file if they conspire with untrusted cloud.

In using advanced de-duplication system supporting authorized duplicate check. In this new de-duplication system, a hybrid cloud architecture is introduced to solve the problem.

Advantage:

By integrating algorithms / techniques we can implement deduplication concepts and reduce the storage cost in a cloud for the data owners.

Secure protocol for anti-collusion attack.

Faster recovery and processing of data.

This would significantly decrease the processing time of load balancer.

Effective and Efficient usage of cloud Storage Space

IX. ALGORITHM

We provide a secure way for key distribution without any secure communication channels, and the users can securely obtain their private keys from group manager 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. 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. 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.

X. SYSTEM DESIGN ANALYSIS

ARCHITECTURE DIAGRAM

The following architecture shows that the cloud storage has many storage areas in which user storeds his file. The admin manage all the activity like maintain the vendors list and revoked user list. The file is stored in the storage area before that it will split into four blocks and the encrypted by two the encryption algorithm RSA and MD-5. After that at the time of downloading the user must request to the file access to the uploading user the admin check the request and grant his request. He send the access key to the requested user throw the mail. The user does not know the encryption pattern.

XI. SYSTEM MODULES DESCRIPTION

AUTHORITY USER VERIFICATION

At first Initial stage all users must create own username and password. After the Registration the user can login to their own space. This application verify the username and password which is either matched or not with the user registration form which is already created by the user while user registration process. If the valid user did not remember the username or password correctly the user can generate own password by using this application.

PRIVACY PRESERVATION

In the Privacy preservation environments, a reasonable security protocol would be developed to achieve the following requirements.

Authentication: A legal user can access its own data fields, only the authorized partial or entire data fields can be identified by the legal user, and any forged or tampered data fields cannot deceive the legal user.

Data anonymity: any irrelevant entity cannot recognize the exchanged data and communication state even it intercepts the exchanged messages via an open channel.

User privacy: any irrelevant entity cannot know or guess a user’s access desire, which represents a user’s interest in another user’s authorized data fields. If and only if the both users have mutual interests in each other’s authorized data fields, the cloud server will inform the two users to realize the access permission sharing.

Forward security: any adversary cannot correlate two communication sessions to derive the prior interrogations according to the currently captured messages.

KEY DISTRIBUTION & ACCESS CONTROL

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 parties.

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.We use the AES algorithm for key generation and encryption.

This algorithm is based on the date stamp + group combination + Group Manger Private Key. Group manager will use this new key and encrypt the file and upload to the cloud

COLLUSION ATTACK

The user leaving a group are termed as revoked users. 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. Thus our proposed system detects the revoked users and protects the data confidentiality and privacy.

SECURE DATA SHARING

Secure data sharing is performed using private keys generated and transmitted using secure communication channels. In our scheme, the users can securely obtain their private keys from group manager Certificate Authorities and secure communication channels using AES algorithm.

CLOUD STORAGE

The group user can upload the files in real cloud server named dropbox. Duplication of files are checked and the files is been uploaded in the cloud server. To get a file, the user needs to send a request to the cloud server. The cloud server will also check the user's identity before issuing the corresponding file to the user. During file access the user key has to match by the group manager the requested file can be downloaded by the group users.

XII. CONCLUSION AND FUTURE WORK

CONCLUSION

In rect, we plan a safe hostile to intrigue information sharing plan for dynamic bunches in the cloud. In our plan, the clients can safely get their private keys from gathering director Declaration Powers and secure correspondence channels. Likewise, our plan can bolster dynamic gatherings proficiently, when another client joins in the gathering or a client is revoked from the group, the private keys of alternate clients don't should be recomputed and updated. In addition, our plan can accomplish secure client revocation, the revoked clients can't have the capacity to get the first information documents once they are revoked regardless of the possibility that they scheme with the untrusted cloud.

FUTURE WORK

In future for solving reliability and scalability issues we further introduce the back-up group manager. In case of any failures of group manager the back up of group manager handles those problems.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, Apr. 2010.

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

[3] 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.

[4] 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.