International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 25 Issue 5 – APRIL 2018 (SPECIAL ISSUE).

PRIVATE KEY AGREEMENT FOR GROUP DATA SHARING IN CLOUD COMPUTING

A.Nandhini[#1], R.Komala*[2] , D.Durgadevi*[3] , K.Indumathi*[4]
*#1, *2, *3 B.TECH (IT), Kings Engineering College, Chennai, India*

*[*4]Assistant professor, Kings Engineering College, Chennai, India*

***ABSTRACT*-Data sharing in cloud computing enables multiple participants to freely share the group data, which improves the efficiency of work in cooperative environments and has widespread potential applications. However, how to ensure the security of data sharing within a group and how to efficiently share the outsourced data in a group manner are formidable challenges. Note that key agreement protocols have played a very important role in secure and efficient group data sharing in cloud computing.In this paper, the group membership is dynamically changed, due to the new user registration and user revocation. Once the user is revoked (exited), the group manager creates the new encryption key for the specific group and transmits in an encrypted format using key agreement algorithm. Second the group manger updates the whole data list in the cloud server. Third the group manages updates the user list and activates the key for access. Finally the user can download and upload with more security using keys.**

Key words: Data sharing, Security, Encryption Key

I. INTRODUCTION

Cloud Computing is a technology which depends on sharing of computing resources than having local servers or personal devices handle the applications. In Cloud Computing, the word "Cloud" means "The Internet", so Cloud Computing means a type of computing in which services are delivered through the Internet. Cloud computing and cloud storage have become hot topics in recent decades. The cloud server provides an open and convenient storage platform for individuals and organizations, but it also introduces security problems. For instance, a cloud system may be subjected to attacks from both malicious users and cloud providers. In these scenarios, it is important to ensure the security of the stored data in the cloud. Several schemes were proposed to preserve the privacy of the outsourced data. The above schemes only considered security problems of a single data owner. However, in some applications, multiple data owners would like to securely share their data in a group manner. Therefore a protocol that supports secure group data sharing under cloud computing is needed. A key agreement protocol is used to generate a common conference key for multiple participants to ensure the security of their later communications, and this protocol can be applied in cloud computing to support secure and efficient data sharing. In cryptography, a key agreement protocol is a protocol in which two or more parties can agree on a key in such a way that both influence the outcome. By employing the key agreement protocol, the conferees can securely send and receive messages from each other using the common conference key that they agree upon in advance. Specifically, a secure key agreement protocol ensures that the adversary cannot obtain the generated key by implementing malicious attacks, such as eavesdropping. Thus, the key agreement protocol can be widely used in interactive communication environments with high security requirements (e.g., remote board meetings, teleconferences, collaborative workspaces, radio frequency identification cloud computing and so on).

II. RELATED WORK

[1]Trust Enhanced Cryptographic Role-based Access Control for Secure Cloud Data Storage **t**o protect the privacy of data stored in the cloud, cryptographic role-based access control (RBAC) schemes have been developed to ensure that data can only be accessed by those who are allowed by access policies. However these cryptographic approaches do not address the issues of trust. In this

paper, we propose trust models to reason about and improve the security for stored data in cloud storage systems that use cryptographic RBAC schemes. The trust models provide an approach for the owners and roles to determine the trustworthiness of individual roles and users respectively in the RBAC system.[2]Yonggang Wen proposed Private Data Deduplication Protocols in Cloud StorageIn this paper, a new notion which we call private data deduplication protocol, a deduplication technique for private data storage is introduced and formalized..[3]Kaiping Xue proposed Dynamic Secure Group Sharing Framework in Public Cloud Computing propose a novel secure group sharing framework for public cloud, which can effectively take advantage of the Cloud Servers' help but have no sensitive data being exposed to attackers and the cloud provider. The framework combines proxy signature, enhanced *TGDH* and proxy re-encryption together into a protocol.[4]Saurabh I. Patil proposed Hybrid Cloud Approach for Secure Authorized Deduplication To better protect data security, this paper makes the first attempt to formally address the problem of authorized data deduplication. Different from traditional deduplication systems, the differential privileges of users are further considered in duplicate check besides the data itself.[5]S.Sherman proposedSecure Cloud Storage Meets with Secure Network CodingThis paper reveals an intrinsic relationship between secure cloud storage and secure network coding for the first time.It is well known that data sharing in cloud computing can provide scalable and unlimited storage and computational resources to individuals and enterprises. However, cloud computing also leads to many security and privacy concerns, such as data integrity, confidentiality, reliability, fault tolerance and so on. Note that the key agreement protocol is one of the fundamental cryptographic primitives, which can provide secure communication among multiple participants in cloud environments.

III. ISSUES IN CLOUD

The main problem in cloud computing faces is preserving confidentiality and integrity of data in aiding data security. The primary solution for theses problem is encryption of data stored in cloud. However, encryption of data also brings up new problem. One of the major problem faced by cloud system since the information is stored at a remote location that the service provider has full access. Therefore; there has been some method of preserving the confidentiality of data stored in the cloud .The main method used to preserve data confidentiality is data encryption.

IV. SYSTEM ARCHITECTURE

The architecture aims to provide the high bandwidth and low delay to the end user. It managing the information between admin and user. It process user request (uploading file, downloading file). Admin generate unique private key for individual user.

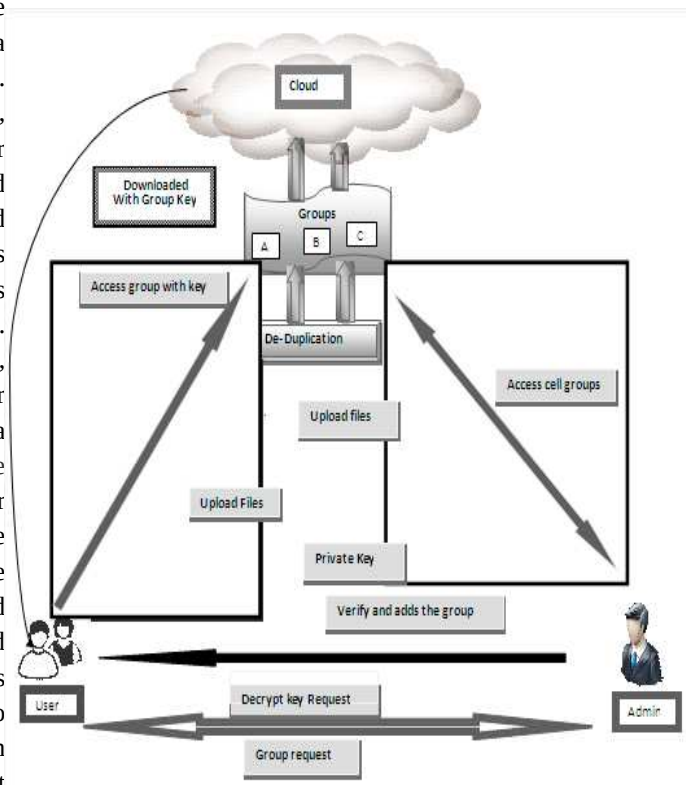

Fig 1. System Architecture

MODULES:

1. Authority User Verification
2. Privacy-preserving
3. Key distribution &Access control
4. Collusion attack
5. Secure data sharing
6. Cloud storage

1. 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.

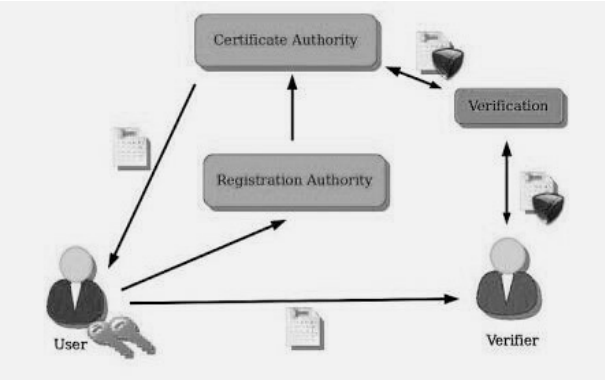

Fig 2. User Verification

If the valid user did not remember the username or password correctly the user can generate own password by using this application.

2. PRIVACY-PRESERVING:

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.

3. KEY DISTRIBUTION & ACCESS CONTROL:

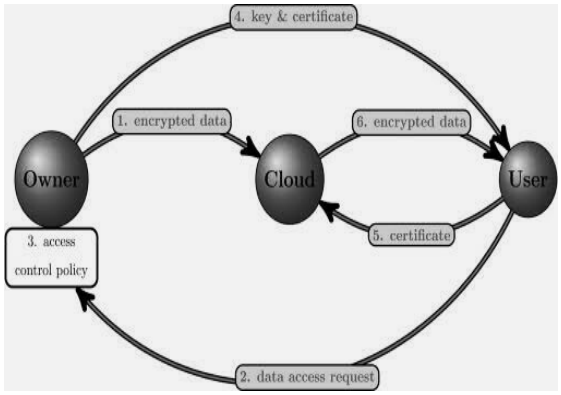

Fig 3. Key Distribution

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 Key Agreement 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.

4. COLLUSION ATTACK:

The users 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.

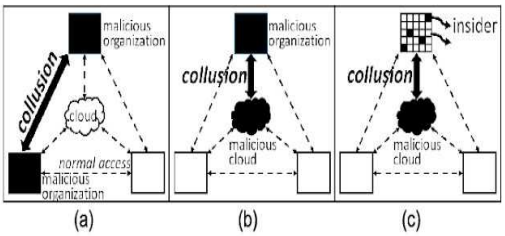

Fig 4. Collusion Attack

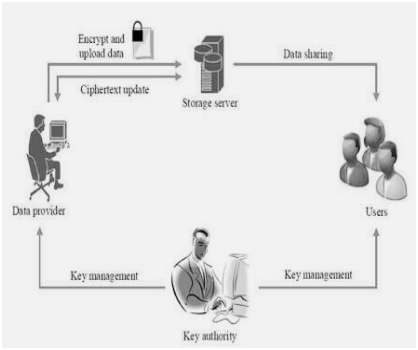

Fig 5. Key Management

5. 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 **Key Agreement Algorithm.**

6.CLOUD STORAGE

The group user can upload the files in real cloud server named drop box. 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.

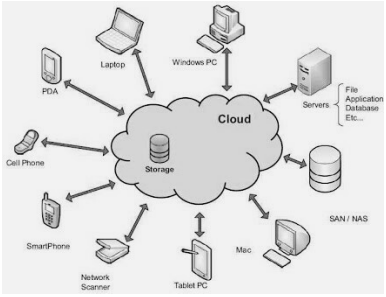

Fig 6. Cloud Storage

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 and the requested file can be downloaded by the group users.

V. CONCLUSION

As a development in the technology of the Internet and cryptography, group data sharing in cloud computing has opened up a new area of usefulness to computer networks. With help of conference key agreement protocol, the security and efficiency group data sharing in cloud computing can be greatly improved. Specifically, the outsourced data of the data owners encrypted by the common conference key are protected from the attacks of adversaries. Compared with conference key distribution, the conference key agreement has qualities of higher safety and reliability. In this paper, we present a novel block design-based key agreement protocol that supports group data sharing in cloud computing. Due to the definition and the mathematical descriptions of the structure of a (v, k + 1, 1)- design, multiple participants can be involved in the protocol and general formulas of the common conference key for participant are derived. Moreover, the introduction of volunteers enables the presented protocol to support the fault tolerance property, thereby making the protocol more practical and secure. In future work, we would like to extend our protocol to provide more properties (e.g., anonymity, traceability, and so on) to make it applicable for a variety of environments.

REFERENCE

[1] L. Zhou, V. Varadharajan, and M. Hitchens, "Cryptographic rolebased access control for secure cloud data storage systems," Information Forensics and Security IEEE Transactions on, vol. 10, no. 11, pp. 2381–2395, 2015.

[2] F. Chen, T. Xiang, Y. Yang, and S. S. M. Chow, "Secure cloud storage meets with secure network coding," in IEEE INFOCOM, 2014, pp. 673–681.

[3] D. He, S. Zeadally, and L. Wu, "Certificateless public auditing scheme for cloud-assisted wireless body area networks," IEEE Systems Journal, pp. 1–10, 2015.

[4] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976.

[5] J. Shen, H. Tan, S. Moh, I. Chung, and J. Wang, "An efficient rfid authentication protocol providing strong privacy and security," Journal of Internet Technology, vol. 17, no. 3, p. 2, 2016.

[6] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Vanstone, "An efficient protocol for authenticated key agreement,"Designs Codes and Cryptography, vol. 28, no. 2, pp. 119–134, 2010.

[7] X. Yi, "Identity-based fault-tolerant conference key agreement," IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 3, pp. 170–178, 2004.

[8] R. Barua, R. Dutta, and P. Sarkar, "Extending joux's protocol to multi party key agreement (extended abstract Lecture Notes in Computer Science, vol. 2003, pp. 205–217, 2.