FRAMEWORK FOR SECURE DATA SHARING IN DYNAMIC GROUP USING PUBLIC CLOUD

Ms.Sornalatha, Assistant Professor, Computer Science and Engineering Department, Chennai.
Mohammad Samiullah, Computer Science and Engineering Department, Chennai.
Pradeep S, Computer Science and Engineering Department, Chennai.
Vemula Murali Krishna Computer Science and Engineering Department, Chennai.

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. It ensures 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, by taking advantage of the symmetric balanced incomplete block design (SBIBD), we present a novel block design-based key agreement protocol that supports multiple participants, which can flexibly extend the number of participants in a cloud environment according to the structure of the block design. Based on the proposed group data sharing model, we present general formulas for generating the common conference key K for multiple participants. The computational complexity of the proposed protocol linearly increases with the number of participants and the communication complexity is greatly reduced. In addition, the fault tolerance property of our protocol enables the group data sharing in cloud computing to withstand different key attacks.

INTRODUCTION:

PUBLIC KEY CRYPTOGRAPHY:

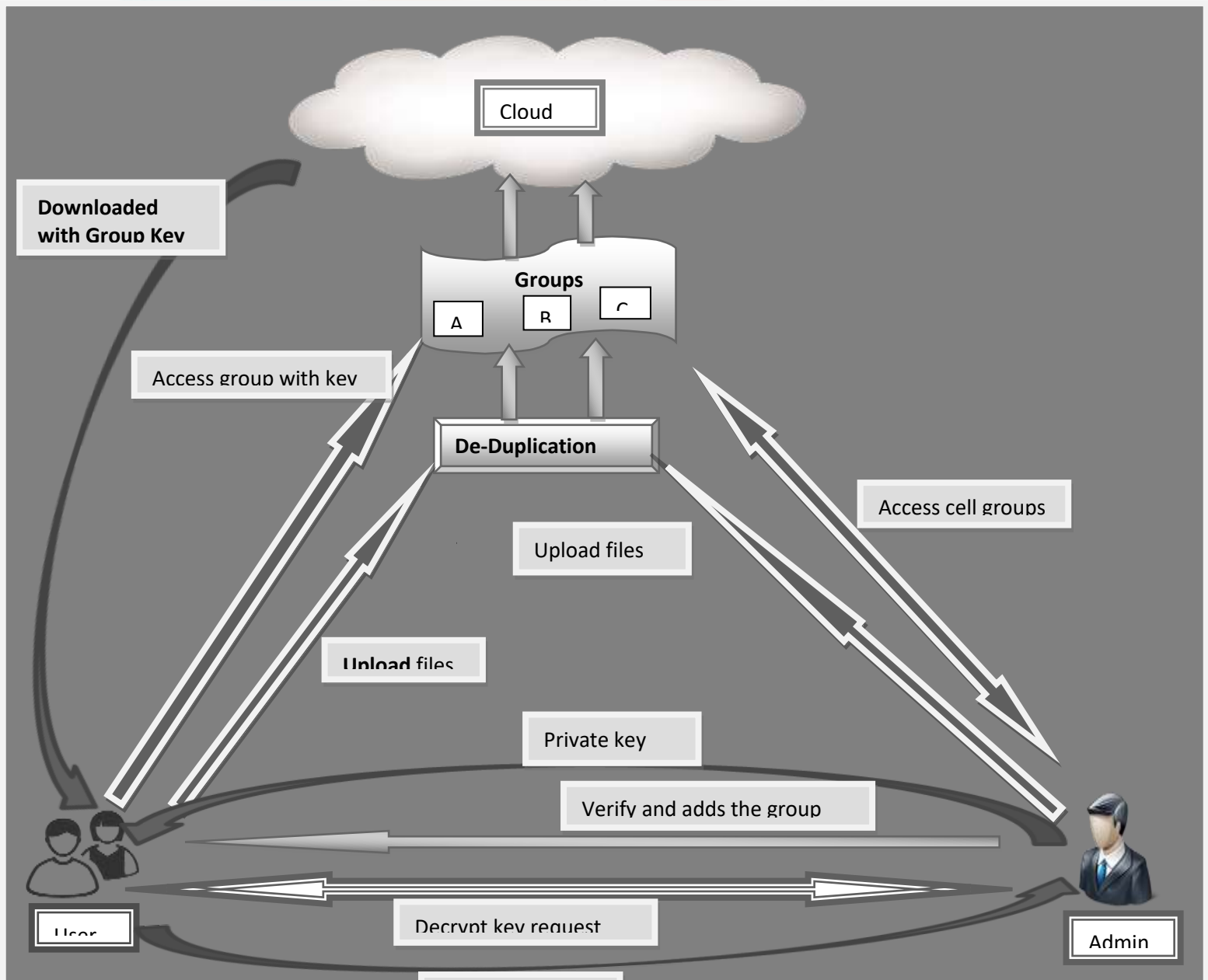
CLOUD computing and cloud storage have become hot topics in recent decades. Both are changing the way we live and greatly improving production efficiency in some areas. At present, due to limited storage resources and the requirement for convenient access, we prefer to store all types of data in cloud servers, which is also a good option for companies and organizations to avoid the overhead of deploying and maintaining equipment when data are stored locally. 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. In 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.

Data sharing in cloud computing enables multiple users 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, by taking advantage of the symmetric balanced incomplete block design (SBIBD), we present a novel block design-based key agreement protocol that supports multiple participants, which can flexibly extend the

number of participants in a cloud environment according to the structure of the block design.

Based on the proposed group data sharing model, we present general formulas for generating the common conference key K for multiple participants. Note that by benefiting of block design, the computational complexity of the proposed protocol linearly increases with the number of participants and the communication complexity is greatly reduced. In addition, the fault tolerance property of our protocol enables the group data sharing in cloud computing to withstand different key attacks

ARCHITECTURE:



WORKING:

At first, We create Web services using Java and this leads to the creation of the new Cloud services. This Cloud consists of humerous data where people can upload their files. To this, it requires an user id and password. This has 3 domains and every domain is maintained by a centralised Group manager which also require their own username and password. After their login, they provide us permission to join the group according to our request. Manager provides the prime credentials to get into our group. Here more security is enhanced and assured because while logging out because the manager will provide the user 9-bit encrypted content. This content will be required for the user to sign out the page. Everytime the user logins, user will be provided with random keys which is not previous as earlier login. Then manager can see the list of people, their usage of resources using MySql.

LIST OF MODULES

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

5.2 MODULE EXPLANATION

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

5.2.2 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.

5.2.3 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 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.

5.2.4 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.

5.2.5 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.**

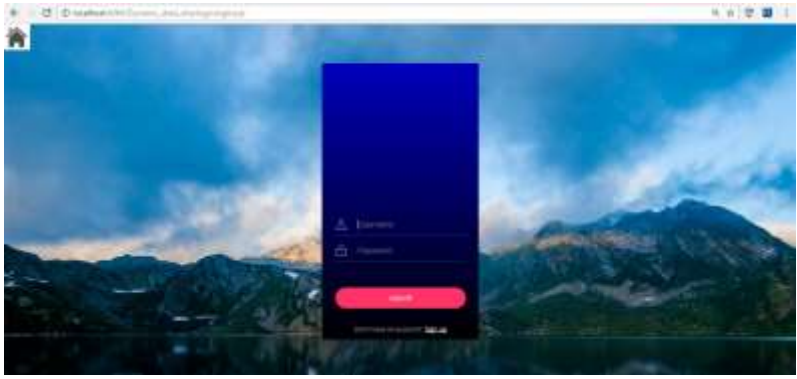
5.2.6 CLOUD STORAGE

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. 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.

HOME PAGE

USER REGISTRATION FORM

USER SIGNIN



USER HOME PAGE

GROUP REQUEST

MANAGER LOGIN

USER DETAILS

FILE REQUEST DETAILS

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 the help of the conference key agreement protocol, the security and efficiency of 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. However, the conference key agreement asks for a large amount of information interaction in the system and more computational cost. To combat the problems in the conference key agreement, the SBIBD is employed in the protocol design. 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 our 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.

REFERENCES

[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.