Block Design-based Key Agreement for Group Data Sharing in Cloud Computing

Ms. P.Adlene Ebenezer, Mr. Sarthak Gupta, Ms Aditi Poddar, Mr. Rahul R

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. Be that as it may, how to guarantee the security of information sharing inside a gathering and how to proficiently share the redistributed information in a gathering way are imposing difficulties. Note that key understanding conventions have assumed a significant job in secure and productive gathering information partaking in distributed computing. In this paper, by exploiting the symmetric adjusted inadequate square plan (SBIBD), we present a novel square plan based key understanding convention that supports different members, which can deftly expand the quantity of members in a cloud domain as indicated by the structure of the square structure. In view of the proposed gathering information sharing model, we present general equations for creating the regular meeting key K for numerous members. Note that by profiting by the (v, k + 1, 1)- square plan, the computational multifaceted nature of the proposed convention straightly increments with the quantity of members and the correspondence intricacy is significantly diminished. What's more, the adaptation to non-critical failure property of our convention empowers the gathering information partaking in distributed computing to withstand distinctive key assaults, which is like Yi's convention.

Key-words
SBIBD-Symmetric Balanced Incomplete Block Design.
PKI-Public Key Infrastructure.

I. INTRODUCTION

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.

II. LITERATURE SURVEY

[1] Cloud data storage has provided significant benefits by allowing users to store massive amount of data on demand in a cost-effective manner. To protect the privacy of data stored in the cloud, cryptographic role-based access control (RBAC) schemes have been developed to ensure that the 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 to improve the security for stored data in cloud storage systems that use cryptographic RBAC schemes.

[2] This paper reveals an intrinsic relationship between secure cloud storage and secure network coding for the first time. Secure cloud storage was proposed only recently while secure network coding has been studied for more than ten years. Although the two areas are quite different in their nature and are studied independently, we show how to construct a secure cloud storage protocol given any secure network coding protocol. This gives rise to a systematic way to construct secure cloud storage protocols. Our construction is secure under a definition which captures the real world usage of the cloud storage. Furthermore, we propose two specific secure cloud storage protocols based on two recent secure network coding protocols

[3] Wireless body area networks (WBANs) consist of many small low-power sensors, through which users could monitor the real-time parameters of patients' physiology remotely. This capability could improve medical care and the monitoring of patients. WBAN devices typically have limited computing, storage, power, and communication capabilities. These limitations restrict the applications that WBANs can support. To enhance the capabilities of WBANs, the concept of cloud-assisted WBANs has been introduced recently. By using cloud computing technologies, cloud-assisted WBANs can provide more efficient processing of patients' physiology parameters and support richer services. In cloud-assisted WBANs, the data of patients'

physiology are stored in the cloud. The integrity of the data is very important because these data will be used to provide a medical diagnosis and other medical treatments.

[4] Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

[5] Providing security and privacy protection in Radio Frequency Identification (RFID) tags is a challenging task due to their highly constrained resources. Because tags cannot support strong cryptography, security must rely on low-computational solutions. Privacy protection is often an additional requirement for acceptance of the technology by end-users. Thus, dedicated lightweight algorithms and protocols need to be designed. In this paper, we propose a set of extremely lightweight (optionally mutual) authentication protocols between a tag and a database (sharing a secret value) which protect the identity of the tag. However, if, for some practical reasons, the identity of the tag needs to be revealed to the reader, an additional optional last step can be added at the end of our protocols to satisfy this requirement.

[6] Authentication and key establishment are fundamental building blocks for securing electronic communication. Cryptographic algorithm for encryption and integrity cannot perform their function unless secure keys have been established and the users know which parties share such keys. It is essential that protocols for providing and key establishment are fit for their purpose. This paper proposes a new and efficient key establishment protocol in the asymmetric (public key) setting that is based on MTI (Matsumoto, Takashima and Imai)-two pass key agreement protocol which consists of three phases; The Transfer and Verification Phase, and The Key Generation Phase. This protocol is strong against most of potential attacks (Known-Key Security, forward (Perfect) Secrecy, Key-Compromise Impersonation, Unknown Key-Share Attack, Small Subgroup Attack, and Man-in-the-Middle Attack) with low complexity (complexity is 4), also it provides authentication between the two entities before exchanging the session keys

III. MODULES

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 verifies 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-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.

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.

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.

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.**

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.

ARCHITECTURE DIAGRAM

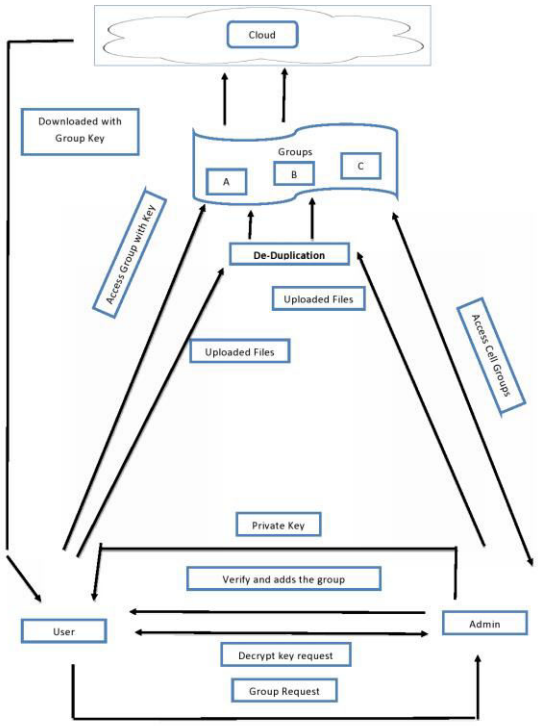

Figure 1.1

IV. TECHNIQUE USED

DIFFIE-HELLMAN ALGORITHM

Elliptic Curve Cryptography (ECC) is an approach to public-key cryptography, based on the algebraic structure of elliptic curves over finite fields. ECC requires a smaller key as compared to non-ECC cryptography to provide equivalent security (a 256-bit ECC security have an equivalent security attained by 3072-bit RSA cryptography).
For a better understanding of Elliptic Curve Cryptography, it is very important to understand the basics of Elliptic Curve. An elliptic curve is a planar algebraic curve defined by an equation of the form

where 'a' is the co-efficient of x and 'b' is the constant of the equation

The curve is non-singular; that is its graph has no cusps or self-intersections (when the characteristic of the co-efficient field is equal to 2 or 3).
In general, an elliptic curve looks like as shown below. Elliptic curves could intersect almost 3 points when a straight line is drawn intersecting the curve. As we can see that elliptic curve is symmetric about the x-axis, this property plays a key role in the algorithm.

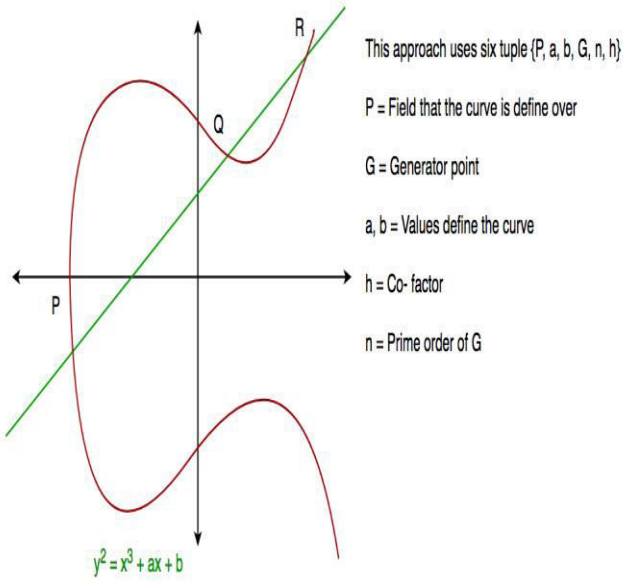

Figure 1.2

The Diffie-Hellman algorithm is being used to establish a shared secret that can be used for secret communications while exchanging data over a public network using the elliptic curve to generate points and get the secret key using the parameters

V. FUTURE WORK

The proxy re-encryption is proposed for feature work, which substitutes most computationally demanding operations to Cloud storage Servers without disclosing any sensitive information or data. The enhanced TGDH scheme permits the group to update the group key pairs using Cloud Servers which does not require all the group members to be online. Proposed scheme provides more efficient, flexible and secured framework for group communication in cloud.

VI. 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.

VII. 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.

[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.