IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

BLOCK DESIGN-BASED KEY AGREEMENT FOR GROUP DATA SHARING IN CLOUD COMPUTING

1. Miss.Vaishali Kashiram Sarkate 2. Dr. Ranu Tuteja

1. Master Of Engineering Student 2. Professor,
Department of Computer Science and Engineering,
Prof. Ram Meghe Institute of Technology and Research, Badnera, India.

Abstract: Data sharing in cloud computing permits a couple of members to freely proportion the institution records, which improves the efficiency of labor in cooperative environments and has big ability applications. However, the way to make certain the safety of records sharing inside a collection and the way to correctly proportion the outsourced records in a collection way are ambitious challenges. Note that key agreement protocols have performed a totally crucial function in steady and green institution records sharing in cloud computing. In this paper, through taking benefit of the symmetric balanced incomplete block design (SBI BD), we gift a singular block design-primarily based totally key agreement protocol that helps a couple of members, that can flexibly enlarge the range of members in a cloud surrounding in accordance to the shape of the block design. Based on the proposed institution records sharing model, we gift a popular formulation for producing the not unusual place convention key K for a couple of members. Note that through making the most of the (v; k + 1; 1)-block design, the computational complexity of the proposed protocol linearly will increase with the range of members and the communiqué complexity is greatly reduced. In addition, the fault tolerance belongings of our protocol permits the institution records sharing in cloud computing to withstand exceptional key attacks, that's much like I's protocol.

Index Term: *Key agreement protocol, symmetric balanced incomplete block design (SBIBD), data sharing, cloud computing.*

I. INTRODUCTION

Cloud computing and cloud storage became hot topics in recent decades. Each is ever-changing the manner we have a tendency to live and greatly improving production potency in some areas. At present, because of restricted storage resources and also the demand for convenient access, we have a tendency to favor to store all types of information in cloud servers, that is additionally a decent possibility for firms and organizations to avoid the overhead of deploying and maintaining equipment when information are keep locally. The cloud server provides an open and convenient storage platform for people and organizations; however it additionally introduces security problems. For instance, a cloud system could also be subjected to attacks from each malicious users and cloud providers. In these scenarios, it is important to confirm the safety of the hold on information within the cloud. In [1], [2], [3], many schemes were projected to preserve the privacy of the outsourced data. The on top of schemes solely thought of security issues of a single information owner. However, in some applications, multiple data homeowners would like to firmly share their information during a cluster manner. Therefore, a protocol that supports secure cluster information sharing underneath cloud computing is needed. A key agreement protocol is used to get a typical conference key for multiple participants to confirm the protection of their later communications, and this protocol is applied in cloud computing to support secure and economical information sharing. Since it absolutely was introduced by Diffie-Hellman in their seminal paper [4], the key agreement protocol has become one in every of the elemental crypto graphical primitives. The fundamental version of the Diffie-Hellman protocol provides an efficient resolution to the matter of making a common secret key between 2 participants. In cryptography, a key agreement protocol may be a protocol within which two or a lot of parties can agree on a key in such the simplest way that each influence the outcome. By using the key agreement protocol, the conferees will firmly send and receive messages from one another using the common conference key that they agree upon in advance. Specifically, a secure key agreement protocol ensures that the resister cannot get the generated key by implementing malicious attacks, similar to eavesdropping. Thus, the key agreement protocol is wide utilized in interactive communication environments with high security necessities (e.g., remote board meetings, teleconferences, cooperative workspaces, frequency identification [5], cloud computing and then on).

The Diffie-Hellman key agreement [4] provides the simplest way to get keys. However, it doesn't offer associate authentication service, which makes it at risk of main-the-middle attacks. This case can be self-addressed by adding some styles of authentication mechanisms to the protocol, as planned by Law et al. in [6]. In addition, the Diffie-Hellman key agreement will solely support 2 participants. Subsequently, to unravel the different key attacks from malicious conferees, who conceive to deliberately delay or destroy the conference, yi planned associate identity-based fault-tolerant conference key agreement in [7].

Currently, several researches are devoted to raise the protection and communication efficiency of the key agreement protocol, that is roofed within the literature [8], [9], [10], [11]. Note that in Chung and Bae's paper [12] and Lee et al.'s paper [13], block style is utilized within the style of associate economical load balance algorithmic rule to keep up load balancing in an exceedingly distributed system. Inspired by [12] and [13], we tend to introduce the symmetric balanced incomplete block style (SBIBD) in planning the key agreement protocol to scale back the quality of communication and computation. As way as we tend to know, the work to design the key agreement protocol with respect to the SBIBD is novel and original.

Motivation

The key agreement protocol is applicable to support data sharing in cloud computing for the following reasons.

1. The generation of a common conference key is performed in a public channel, which is suitable for cloud computing environments.

2. The key agreement protocol can support and provide secure data sharing for multiple data owners within a group, where the data sharing follows a many-to-many pattern. Compared with the one-to-many pattern, the many-to-many pattern in group data sharing provides higher efficiency in the environment of cooperative storage.

3. The key agreement protocol is based on a decentralized model, where a trusted third party is not required. This means that every data owner in a group fairly contributes and determines the common conference key such that the outsourced data are controlled by all the data owners within a group.

Objectives

- To put in force the platform for person on they could upload information and get entry to any time from cloud.
- To share the information from organization to organization or individually.
- To growth the safety with encryption.

II. LITERATURE REVIEW

It is widely known that data sharing in cloud computing can offer scalable and limitless storage and computational sources to people and enterprises. However, cloud computing additionally ends in many protection and privateers concerns, together with records integrity, confidentiality, reliability, fault tolerance and so on. Note that the key agreement protocol is one of the essential cryptographic primitives, which could offer stable communication amongst a couple of members in cloud environments.

F. Chen, T. Xiang, Y. Yang, and S. S. M. Chow [2] had designed a general construction of secure cloud storage protocol based on any secure network coding protocol. However, it is not known if a secure network coding protocol can be constructed from a secure cloud storage protocol. It is an interesting future work to consider under what condition this can be done.

D. He, S. Zeadally , and L. Wu[3] had discussed Cloud-assisted WBANs, which are the integration of a cloud computing platform and WBANs, could bring major benefits (as we discussed earlier) over traditional WBANs. One of the major challenges of a cloud-assisted WBAN is to ensure the integrity of the medical data stored at a cloud server. The auditing technique is an efficient tool for checking the integrity of the data stored remotely. However, previous auditing schemes suffer from key management and key escrow problems. To address these challenges, they proposed a new CLPA scheme. Compared with previously proposed schemes, our CLPA scheme not only can address the security problems in TPKC-based public auditing schemes and ID-based public auditing schemes but also yields better performance. In addition, their proposed CLPA scheme is provably secure in a strong security model, making CLPA very suitable for use in cloud-assisted WBANs.

L. Law, A. Menezes, M. Qu, J. Solinas, and S. Vanstone, [6] shows the comparison includes the basic two-pass protocols. The computational requirements are indicated by counting the number of exponentiations computed by each principal in protocol run and this is the complexity. Also H.Elkamchouchi, M.Eldefrawy works by computing and exchanging two vectors but the new one works and exchanges one value.

In [14] and [15], based on symmetric-key cryptography, several schemes were proposed to enable efficient encryption of the outsourced data. However, encryption keys should be transmitted in a secure channel, which is not possible in practice, particularly in the open cloud environment.

In [16], it was introduced that resistance to compromised keys has been taken into consideration, which an important issue in the context of cloud is computing.

Cloud storage auditing with verifiable outsourcing of key updates paradigm was proposed by Yu et al. in [17] to achieve resistance to compromised keys. In this paradigm, the third party auditor (TPA) takes responsibility for the cloud storage auditing and key updates. In particular, the TPA is responsible for the selection and distribution of the key. The key downloaded from the TPA can be used by the client to encrypt files that he will upload to the cloud. In contrast, the generation and distribution of the key is based on a centralized model in [17], which not only imparts a burden to the TPA but also introduces some security problems.

In [18], a key agreement algorithm was exploited by De Capitani di Vimercati et al. to achieve data access when data are controlled by multiple owners. Therefore, the key agreement protocol can be applied in group data sharing to solve related security problems in cloud computing. Following the first pioneering work for key agreement [4], many works have attempted to provide authentication services in the key agreement protocol.

In [19], a public key infrastructure (PKI) is used to circumvent man-in-the-middle attacks. However, these protocols are not suitable for resource-constrained environments since they require executions of time-consuming modular exponentiation operations.

Key agreement protocols that use elliptic curve cryptography (ECC) have been proposed in [20], [21]. These protocols are more efficient than the protocols that resort to the PKI because point additions or multiplications in elliptic curves are more efficient compared with the modular exponentiation. Moreover, based on the difficulty of solving the elliptic curve discrete logarithm problem (ECDLP), protocols that use ECC are more secure.

To avoid the requirement of the public key certificate, in 1984, identity-based cryptography (IBC) was proposed by Shamir [22]. However, it was not until 2001 that the first practical IBC scheme [10] was proposed by Boneh and Franklin. Due to the strict security proof and high efficiency, this scheme has received widespread recognition in academic fields.

In the same year, a popular proof model for group key establishment was proposed by Bresson et al. [23]. In this protocol, to manage the complexity of definitions and proofs for the authenticated group Diffie-Hellman key exchange, a formal model was presented, where two security goals of the group Diffie-Hellman key exchange were addressed. However, some security properties are missing in [23], which are essential for preventing malicious protocol participants. Note that all the above protocols have been proven and analyzed for security, but some of them can only be applied to the key agreement between two entities and need a large amount of resources to perform calculations.

An identity-based authenticated key agreement protocol was proposed by Shen et al. in [9], which improves the efficiency of the conference key agreement and provides entity authentication services. However, there are some obstacles in Shen et al.'s protocol [9] in real applications. One is that the protocol only discusses a specific situation when the number of conferees is exactly 7. The other is that the protocol does not discuss the general situation and does not provide the key agreement process for multiple participants, which makes the protocol lack flexibility and practicability.

Motivated by the above observation, the key agreement protocol is applicable to support data sharing in cloud computing for the following reasons.

1. The generation of a common conference key is performed in a public channel, which is suitable for cloud computing environments.

2. The key agreement protocol can support and provide secure data sharing for multiple data owners within a group, where the data sharing follows a many-to-many pattern. Compared with the one-to-many pattern, the many-to-many pattern in group data sharing provides higher efficiency in the environment of cooperative storage.

3. The key agreement protocol is based on a decentralized model, where a trusted third party is not required. This means that every data owner in a group fairly contributes and determines the common conference key such that the outsourced data are controlled by all the data owners within a group.

Therefore, this research design a block design-based key agreement protocol for data sharing in cloud computing. First, proposed an algorithm to construct the (v, k + 1, 1)-design. Then, with respect to the mathematical description of the structure of the (v, k+1, 1)-design, general formulas for generating the common conference key K for multiple participants are derived. Namely, the proposed protocol supports multiple participants

III. SYSTEM ANALYSIS

Existing System

This analysis introduced an internet base platform for cluster knowledge sharing in cloud computing. In our existing system there are multiple departments in single organization. Suppose 2 departments needs to try to the speech communication or exchange messages or files with every other. Then 1st of all they need to do the key agreement. These all activities are done beneath the watch of TPA. Shut in if the privacy breaks then TPA sends warning message to the user likewise as cloud server.

Key Agreement Protocol

In cryptography, a key-agreement protocol could be a protocol whereby 2 or additional parties will agree on a key in such the way that each influence the outcome. If properly done, this precludes unwanted third parties from forcing a key alternative on the agreeing parties. Protocols that are helpful in follow additionally don't make known to any eavesdropping party what key has been united upon.

Hardware and Software Requirements

Minimum Hardware Requirement

- System: Core i5 1.80 GHz Processor
- Hard Disk: 500 GB.
- Ram: 4 GB.

Software Requirement

- Operating System : Windows 7
- Technology Used: PHP
- Database Used : Mysql

IV. SYSTEM DESIGN

Data flow diagram

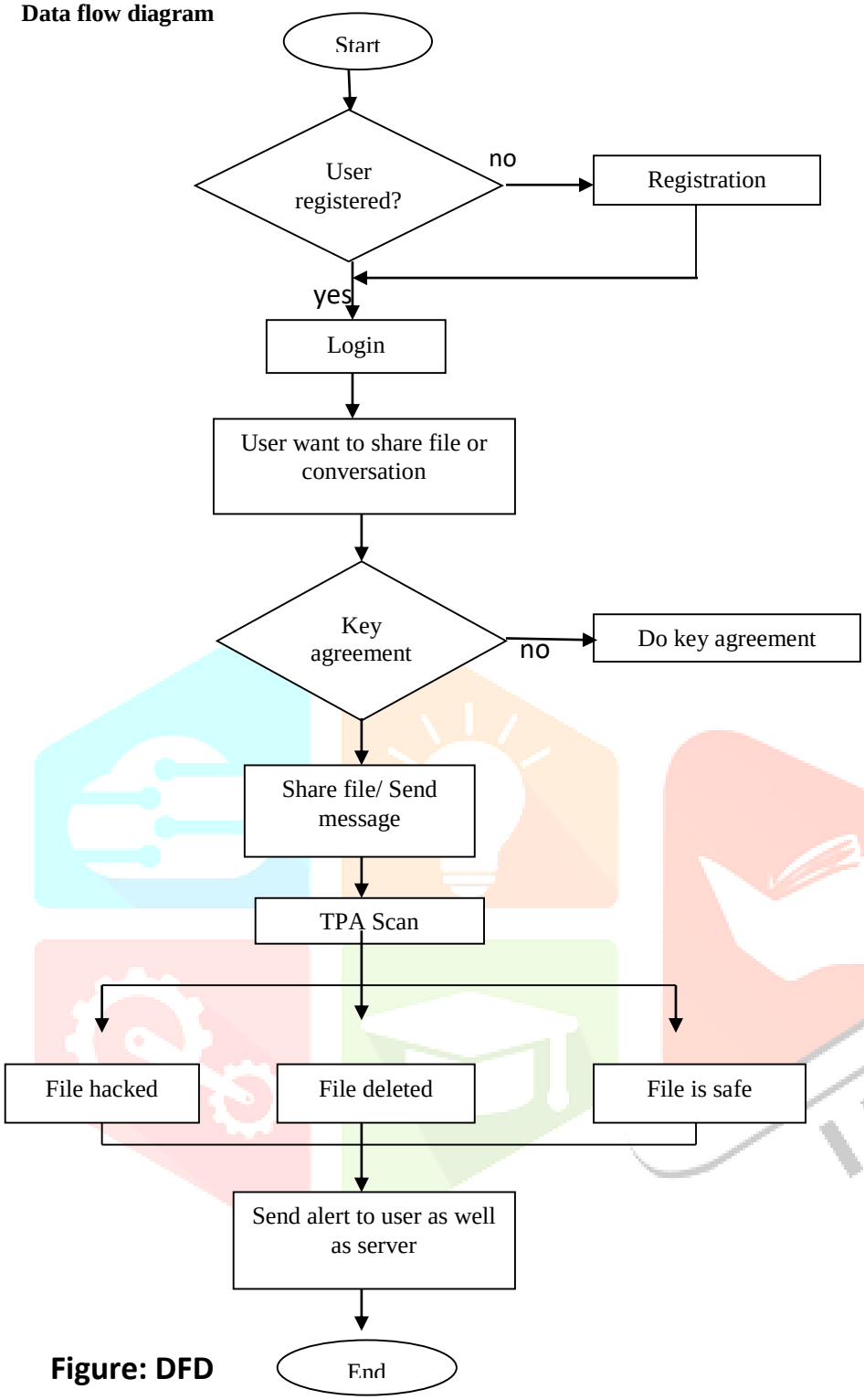

Figure: DFD

Methods

The construction of the group data sharing model to support a group data sharing scheme for multiple participants applying an SBIBD, we design an algorithm to construct the (v, k + 1, 1)-design. Moreover, the constructed (v, k + 1, 1)-design requires some transformations to establish the group data sharing model such that v participants can perform the key agreement protocol. 4.1 Construct the (v, k + 1, 1)-design in our group data sharing model, the parameters of the SBIBD have some specific meanings. In a (v, k+1, 1)-design, v denotes the number of participants and the number of blocks. Every block embraces k + 1 participant, and every participant appear k + 1 times in these v blocks. Furthermore, every two participants appear simultaneously in exactly one of the v blocks. Following papers [12] and [13], Algorithm 1 is designed to construct the structure of a (v, k + 1, 1)-design. First, a prime number k is selected. Then, the number of participants is determined by the value of k, which is computed as v = k 2 + k + 1†. Finally, according to Definition 3, V = {0, 1, 2... v − 1} represents the set of v participants, whereas B = {B0, B1, B2... Bv−1} implies v blocks constituted by these v participants. Note that the block is defined as Bi = {Bi,0, Bi,1, Bi,2, ..., Bi,k}, which means each block embraces k + 1 participants, and Bi,j denotes which participant is contained in the j th column of the i th block.

Sometimes we will consider blocks organized as a matrix in which column j is composed by elements Bi, j for i = 0, 1, 2... K and row i is composed by elements Bi, j for j = 0, 1, 2... k. The structure of the (v, k + 1, 1)-design is constructed by Algorithm 1, which outputs numbers Bi, j for i = 0, 1, ..., k2 + k and j = 0, 1, ..., k. In Algorithm 1, the notation MODk represents the modular operation that takes the class residue as an integer in the range 0, 1, 2... K − 1. Based on Algorithm 1, we can create the structure of a (v, k + 1, 1)-design that involves v participants. Moreover, Algorithm 1 can directly determine which participant should be involved in each block. For example, taking the (13, 4, 1)-design into consideration, where 13 participants are involved in this structure, we can decide which participant should be contained in the 3 rd column of the 8 th block by computing B7,2 = jk + 1 + MODk(i − j + (j − 1) b(i − 1)/kc) = 2 • 3 + 1 + MOD3(7 − 2 + (2 − 1) b(7 − 1)/3c) = 7 + MOD3(5 + 1 • 2) = 7 + 1 = 8. Therefore, from the above calculation, it is concluded that participant 8 is contained in the 3 rd column of the 8th block. Here, participant represents the I th participant.

Algorithm: Generation of a(v, k+1, 1)-design
for i = 0; i ⩽ k; i + + do
for j = 0; j ⩽ k; j + + do
if j == 0 then
Bi,j = 0;
Else
Bi, j = ik + j;
end if
end for
end for
for i = k + 1; i ⩽ k 2 + k; i + + do
for j = 0; j ⩽ k; j + + do
if j == 0 then
Bi, j = b(i − 1) /kc;
else Bi,
j = jk + 1 +MODk (i−j + (j −1) b (i − 1)/kc);
end if
end for
end for

Algorithm is an optimization of the algorithm in [12] and the proof of the correctness follows the same lines than the proof in [12] and [13]. The structure created by Algorithm 1 can be proven to satisfy the conditions of the (v, k + 1, 1)-design, which means that each participant of V appears exactly k + 1 times in B and that each pair of participants of V appears exactly once in B. These properties can be utilized to design the group data sharing model, which can diminish the communication cost of the proposed protocol.

V. CONCLUSION

As a development within the technology of the net and cryptography, cluster information sharing in cloud computing has unfolded a brand new space of quality to pc networks. With the assistance of the conference key agreement protocol, the safety and potency of cluster information sharing in cloud computing are often greatly improved. Specifically, the outsourced data of the information homeowners encrypted by the common conference key are protected against 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 knowledge interaction within the system and a lot of procedure cost. To combat the issues within the conference key agreement, the SBIBD is employed within the protocol design. during this paper, we have a tendency to gift a unique block design-based key agreement protocol that supports cluster information sharing in cloud computing. because of the definition and therefore the mathematical descriptions of the structure of a (v, k + 1, 1) design, multiple participants are often concerned within the protocol and general formulas of the common conference key for participant are derived. Moreover, the introduction of volunteers permits the conferred protocol to support the fault tolerance property, thereby creating the protocol a lot of sensible and secure. In our future work, we might prefer to extend our protocol to produce a lot of properties (e.g., anonymity, traceability, so on) to form it applicable for a variety of environments.

VI. REFERENCES

[1] Jian Shen, Tianqi Zhou, Debiao He, Yuexin Zhang, Xingming Sun, and Yang Xiang, “Block Design-based Key Agreement for Group Data Sharing in Cloud Computing,” IEEE Systems Journal, 2017.

[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, “Certificate less 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, 2003.

[9] J. Shen, S. Moh, and I. Chung, "Identity-based key agreement protocol employing a symmetric balanced incomplete block design," Journal of Communications and Networks, vol. 14, no. 6, pp. 682–691, 2012.

[10] B. Dan and M. Franklin, "Identity-based encryption from the wail pairing," Siam Journal on Computing, vol. 32, no. 3, pp. 213–229, 2003.