A Survey on Data Sharing using Block Design-based Key Agreement in Cloud Computing

Miss. Sayali Sanjay Deshmukh[1], Prof. Shrinivas Sonkar [2]
P.G.Student, Department of Computer Engineering[1], Head of Department, Department of Computer Engineering[2],
Amrutvahini College of Engineering, Sangamner,MH,India[1] Amrutvahini College of Engineering, Sangamner, MH, India[2]

Abstract: ***Cloud computing allows multiple participants to share their data and helps improve work efficiency. The key agreement protocol is important in group data sharing and ensures security and efficiency. A block design-based key agreement protocol is put forth using symmetric balanced incomplete block design that supports multiple participants and is helpful in flexibly increasing the participants in the cloud environment using the block design structure. The different types of key attacks can be avoided using the fault tolerance property of the protocol.***

Keywords: ***Key agreement protocol, Data sharing, Cloud storage.***

I. INTRODUCTION

Cloud computing and cloud storage have become hot topic of discussion these days. Cloud computing has changed the way of living and improving the production efficiency. Due to limited resources for data storage and for the ease of convenience it is preferred to store all type of data in servers provided by the cloud. Cloud serves a better option to store different type of the data for organization and companies reducing their overhead of maintaining the equipment and the infrastructure. But the storage gives rise to the different security problems. The data stored on cloud may not be safe and it can be attacked by the cloud providers and the malicious participants or the users. The prior schemes only considered single data owners security problems. Using this key agreement protocol a common conference key is generated for different participants to communicate securely, this can be applied for data sharing in cloud computing to provide security and efficiency. But storage gives rise different security problems. The data stored on cloud may not be that safe and can be even attacked by the cloud providers and malicious participants or users. The prior schemes considered single data owners security problems. Using key agreement protocol common a conference key is generated for the multiple participants to communicate securely, which can be applied for data sharing in cloud computing to provide the security and efficiency. In the key agreement protocol two or more number of participants can agree on a key. The key agreement protocol is thus employed to ensure the security while sending and receiving messages among groups using common conference key. The key agreement protocol helps to ensure that the generated key cannot be obtained by adversary.

II. LITERATURE SURVEY

Communication security is provided to different participants in cloud by the key agreement protocol which is cryptographic basic. Based on the symmetric key cryptography in [1] and [2] different schemes were proposed to ensure the efficient encryption of the outsourced data. An important issue of the resistance to compromised keys was introduced in [3]. To achieve the resistance to the compromised keys , in [4] auditing of cloud storage with the verifiable outsourcing of the key updates model was proposed, in which third party auditor (TPA) is responsible for auditing and updates of the cloud storage. The key is been selected and then distributed by the TPA. This key is then used by the clients for encrypting the files which will be uploaded to cloud. A key agreement protocol was introduced in [5] to achieve the data access as the data is controlled by the multiple owners. The problems related with the security are solved by key agreement protocol and it is then applicable for sharing the data within group in cloud. In [6] multiple attempts were made in key agreement protocol to provide the services related to the authentication. In [7] a public key framework have been used to resist the man-in-middle attacks. An identity based cryptography was proposed by [8] to avoid public key certificate requirements. Recently in [9] an identity- based key agreement protocol was proposed which provided authentication services to these entities and the key agreement efficiency. The above protocols have great efficiency than protocols that work on the public key infrastructure. There are some number of obstacles in above work. The situation in which user participating in the group is seven is discussed by the protocol and not regular situation. Thus, this protocol lacks in the practicability and the flexibility.

III. PROPOSED SYSTEM OVERVIEW

The system consists of the block design based on the symmetric balanced incomplete block design. It has (v, $k+1$, 1) design on which the exchange of information is based, where v is number of participants, k is the prime number and k is the number of participants in each block. The expected messages of both the sender and the receiver are resolved by each member of group based on the (v, $k+1$, 1) design. The (v, $k+1$, 1) design constructs a decentralized model. We establish a group data sharing model based on the symmetric balanced incomplete block design which determines way of communication among the participants of group. The protocol performs fault detection ensuring that the common conference key is generated among all participants of group. The fault detection replaces malicious participant to support the fault detection property. It resists all possible key attacks making group data sharing more efficient and secure. Using key agreement protocol in a group can be formed by the multiple participants to share data efficiently by symmetric balanced incomplete block design. A key agreement is performed by each participant within group to derive common conference key ensuring security of data outsourced. The participants of a group generate common conference key. This generated key cannot be accessed by an attacker or the semi-trusted cloud server.

Due to the following reasons of data sharing uses key agreement protocol :

- The generation of the common conference key is performed within public channel.
- Secure data sharing among the multiple data owners within the group is supported by key agreement protocol.
- A many-to-many pattern for group data sharing is provided by protocol which provides efficient organizational storage.
- On the decentralized model the protocol is based upon.
- The common conference key is contributed and then determined by each member of group.
- Each member of group controls data that is been outsourced.

The system model includes of the cloud, the TPA and the users in group data sharing scheme. Cloud is the semi-trusted party which gives the data storage and download services to users. TPA performs the cloud storage auditing, generation of the system parameters and the fault detection. The group is formed to work together to share data and upload the data to the cloud server. The users can be an individual or group of individuals. The user can be an android device, mobiles, laptops, nodes in the underwater sensors. This model is based on the symmetric balanced incomplete block design. All the participants within a group exchange messages according to symmetric balanced incomplete block design to determine the common conference key. The adversaries are included in protocol. The adversaries can be active or passive. An active adversary is an individual who impersonates participant or disturbs conference. The passive adversary is an individual who attempt to gain information about conference key from multicast channel by performing eavesdropping. The participants define correctness of common conference key. The participants within group are responsible for generating and updation of conference key. The capabilities and actions of attacker are determined by adversaries. The participants are impersonated by adversary. In the conference a long term secret key of participant is revealed by adversary. The information about session key of the new participant is also learnt by adversary.

The key agreement protocol consists of three different phases:

a) Initial Phase

In this phase of the protocol, the third party auditor is responsible for generating the system parameters and distribution of private key to all participants.

b) Key Agreement Phase

Two rounds are required in this phase. The generation of a common conference key for all members in group and exchange of the messages is performed by the rounds.

c) Fault Detection Phase

This phase prevents the different key attacks from malicious participants. This phase is important as we cannot guarantee that all participants present in group are honest and they can destroy conference. The third party auditor ensures that each of the participant generates unique key to prevent the delaying of conference. A block design based key agreement protocol is designed for the data sharing within the group.

IV. ALGORITHMS DESIGN

First algorithm, constructs the (*v, k+1, 1*) design and the second algorithm reconstructs block design formed in the first algorithm. The proposed key agreement protocol supports the multiple participants for group data sharing.

Algorithm 1 : Construction of (v,k+1,1) block

In symmetric balanced incomplete block design each parameter has its meaning. In *(v,k+1,1)* design, number of blocks and participant is denoted by *v, k* is a prime number. Every block contains *k+1* participants and there is *k+1* times appearance of each participant in every block.

1. A prime number k is selected.
2. The value of k determines the number of participants.
3. Set of v participants is represented by V = {0, 1, 2,…, v-1} .
4. The v blocks constituted by these v participants is implied by B = {B0,B1,…,Bv-1} .
5. Perform modular operation on each block element.
6. Until (v, k+1,1) block design is constructed.

Algorithm 2 : Reconstruction of block

For generation of conference key for every participant *(v, k+1,1)* design must have property that each block contains every participant.

Thus, there is need of the reconstruction and here we transform B to E and then B is formed in algorithm 1. This reconstructed block E is then used to design group data sharing model for users. Thus, the common conference key can be generated and key agreement protocol can be then processed.

1. Transform first k+1 blocks in B to first k+1 blocks in E.
2. Element 0 appears k+1 times in first column and remaining elements appear once.
3. At last the transformation of remaining k+1 blocks in B to k.(k-1) blocks of E is performed..

V. CONCLUSION

The performance and the security of the group data sharing has been improved using the conference key agreement protocol. The stored data of the data owners is given the protection from different attacks of the adversaries by encryption using a common conference key. Higher the safety and the reliability are provided by conference key agreement protocol. In a group data sharing model in the cloud computing the block design-based key agreement protocol is presented.

REFERENCES

[1] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: Improved definitions and efficient constructions,” Journal of Computer Security, vol. 19, no. 5, pp. 79–88, 2011.

[2] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-preserving multi-keyword ranked search over encrypted cloud data,” IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 222–233, 2014.

[3] J. Yu, K. Ren, C. Wang, and V. Varadharajan, “Enabling cloud storage auditing with key-exposure resistance,” IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1–1, 2015.

[4] J. Yu, K. Ren, and C. Wang, “Enabling cloud storage auditing with verifiable outsourcing of key updates,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1–1, 2016..

[5] S. D. C. D. Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, “Encryption policies for regulating access to outsourced data,” Acm Transactions on Database Systems, vol. 35, no. 2, pp. 78–78, 2010.

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

[7] H. Guo, Z. Li, Y. Mu, and X. Zhang, "Cryptanalysis of simple three-party key exchange protocol," Computers and Security, vol. 27, no. 1-2, pp. 16–21, 2008.

[8] A. Shamir, "Identity-based cryptosystems and signature schemes," Lecture Notes in Computer Science, vol. 21, no. 2, pp. 47–53, 1985.

[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.