International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST

Group Data Sharing in Cloud Computing with Secure Key Agreement Modal

Wajiha Nausheen*[1], Shital Gaikwad[2]
*[1]PG Student, Computer Science and Engineering, MPGI, Nanded, Maharashtra, India
[2]Associate Professor, Computer Science and Engineering, MPGI, Nanded, Maharashtra, India

Article Info
Volume 8, Issue 4
Page Number : 500-504

Publication Issue
July-August-2021

Article History
Accepted : 02 Aug 2021
Published : 10 Aug 2021

ABSTRACT

Cloud computing is said to be the service-oriented computing technology, which are affordable and flexible over the internet. In past few years the cloud has become more matured and provided many services, one of the primary services is data sharing in Group, where the data can be easily shared from one member to another. However, while sharing the data security is one of the primary concerns. In past several methodologies has been proposed. However, these methods lacked from the feasibility. Hence, in this paper we have proposed methodology is based on the selection scheme. Here General Group Key is generated and moreover General Key agreement protocol is decentralized based model where the data are controlled by the owner within the same group. Moreover, the proposed methodology is evaluated by analyzing the comparative analysis based on the various number of parameters. Result Analysis suggests that our methodology simply outperforms the existing one. 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. We proposed a block design based key agreement protocol in which, TPA find malicious user from group and remove from group we have a tendency to gift general formulas for generating the common conference key K for multiple participants. Note that by taking advantage of the (v; k + 1; 1)-block design, the computational complexity of the planned Protocol linearly will increase with the quantity of participants and also the communication quality is greatly reduced. Additionally, the fault tolerance property of our protocol allows the group data sharing in cloud computing to face up to different key attacks that are analogous to Yi's protocol.

Keywords : Group Data Sharing, Cloud Computing

I. INTRODUCTION

In cryptography, a key-agreement protocol is a protocol whereby two or more parties can agree on a key in such a way that both influence the outcome. If properly done, this precludes undesired third parties from forcing a key choice on the agreeing parties. Protocols that are useful in practice also do not reveal to any eavesdropping party what key has been agreed

upon. Many key exchange systems have one party generate the key, and simply send that key to the other party -- the other party has no influence on the key. Using a key-agreement protocol avoids some of the key distribution problems associated with such systems. Protocols where both parties influence the final derived key are the only way to implement perfect forward secrecy. Cloud computing and cloud storage has become hot topics in recent decades. Every area unit dynamical the method we tend to live and greatly improve. At present, thanks to restricted storage resources and also the demand for convenient access, we tend to choose to store every kind of information in cloud servers that is additionally a decent choice for firms and organizations to avoid the overhead of deploying and maintaining instrumentation once information area unit hold on domestically. The cloud server provides associate open and convenient storage platform for people and organizations; however it additionally introduces security issues. a cloud system is also subjected to attacks from each malicious users and cloud suppliers. 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. Since it was introduced by Diffie-Hellman in their seminal paper, the key agreement protocol has become one of the fundamental cryptographic primitives The basic version of the Diffie-Hellman protocol provides an efficient solution to the problem of creating a common secret key between two participants. In cryptography, a key agreement protocol is a protocol in which two or more parties. 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).we present an efficient and secure block design-based key agreement protocol by extending the structure of the SBIBD to support multiple participants, which enables multiple data owners to freely share the outsourced data with high security and efficiency. Note that the SBIBD is constructed as the group data sharing model to support group data sharing in cloud computing. Moreover, the protocol can provide authentication services and a fault tolerance property. This paper area unit summarized as follows. Secure cluster information sharing in cloud computing is supported by the protocol. in step with the information sharing model applying the SBIBD, multiple participants will type a gaggle to expeditiously share the outsourced information. Later, every cluster member performs the key agreement to derive a typical conference key to confirm the protection of the outsourced cluster information. Note that the common conference secret's solely created by cluster members. Attackers or the semi-trusted cloud server has no access to the generated key. Thus, they cannot access the initial outsourced information (i.e., they solely acquire some unintelligible data). Therefore, the projected key agreement protocol will support secure and

economical cluster information sharing in cloud computing.

II. METHODOLOGY

Several security schemes for data sharing on untrusted servers have been proposed. In these approaches, data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively. By setting a group with a single attribute, we proposed a secure provenance scheme based on the cipher text-policy attribute-based encryption technique, which allows any member in a group to share data with others. However, the issue of user revocation is not addressed in their scheme. Presented a scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique. Unfortunately, the single owner manner hinders the adoption of their scheme into the case where any user is granted to store and share data.

Disadvantages:

1. It does not provide security for sharing the data within the groups.
2. It does not provide privacy preserving access control to the users. In this paper , by taking advantage of the isobilateral balanced incomplete block vogue (SBIBD), we've got an inclination to gift a very distinctive block design-based key agreement protocol that supports multiple participants, which could flexibly extend the quantity of participants in associate extremely

cloud setting in step with the structure of the block vogue. Supported the projected cluster info sharing model, we've got an inclination to gift general formulas for generating the common conference key K for multiple participants. Note that by creating the foremost of the (v; k + 1; 1)-block vogue, the procedure quality of the projected protocol linearly can increase with the quantity of participants and thus the communication quality is greatly reduced. in addition, the fault tolerance property of our protocol permits the cluster info sharing in cloud computing to set about to all totally different key attacks. A key agreement protocol is used to return up with a customary conference key for multiple participants to create positive the security of their later communications, and this protocol is applied in cloud computing to support secure and economical info sharing.

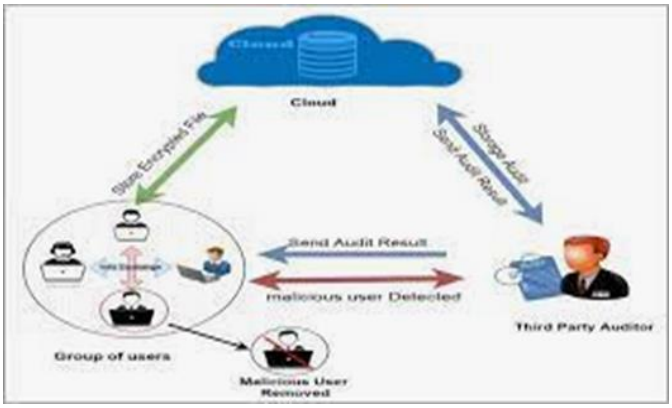

Figure. 1: System Architecture

Advantages: 1) we present a novel block design-based key agreement protocol that supports multiple participants 2) flexibly extend the number of participants in a cloud environment according to the structure of the block design.

III. MODELING AND ANALYSIS

The Mathematical Model used in this paper is given below:

1) Let S beasystem. S={I,O,P,F,s,Ic}

2)IdentifysetofinputsI

LetI={SetofoutsourceddatasetsbycorrespondingdatauseR}

3) IdentifysetofoutputasO
LetO={Securely data sharing with group participant and remove malicious user from group through TPA}
4) Identify the set of processes as P P={TPA,B,V,K, F, ei , di ,H1,H2 } TPA=ThirdPartyAuditor. B=Set of block. V=No of group participant. K=.Key Agreement. F=FaultTolerance ei= PublicKey di = PrivateKey H1,h2=HashFunction5.IdentifyfailurecasesasF
F={share data to malicious user in group.}
5) Identifysuccessass s={share data in group and give private key to all group participant and remove malicious user from group.} 6) Identify the initial condition Ic
Ic={Outsourceddatawithitsprivacyprivilegestobemaint ain and Material which are used is presented in this section. Table and model should be in prescribed format. Here we can analyse that we have been using hash functions for generating keys. Before user enters he/she is verified from the TPA. After that user has been verified with help of hash function we are generating securities keys.W are even sharing data in the group and providing private keys to all group participants and their we are removing malicious users from the group. Proposed Algorithm (AES Algorithm) broadly speaking the encryption/decryption can be done via symmetric key or asymmetric key In symmetric algorithms, both parties share the secret key for both encryption/decryption, and from privacy perceptive it is important that this key is not compromised, because cascading data will then be compromised.
Symmetric encryption/decryption requires less power for computation. On the other hand asymmetric algorithms use pairs of keys, of which one key is used for encryption while other key is used for decryption. Generally the private key is kept secret and generally held with the owner of data or trusted 3rd party for the data, while the public key can be distributed to others for encryption. The secret key can't be obtained from the public key Steps Step 1: Start Step 2: Derive the set of round keys from the cipher key. Step 3: Initialize the state array with the block data (plaintext) Step 4: Add the initial round key to the starting state array. Step 5: Perform the tenth and final round of state manipulation. Step 6: Copy the final state array out as the encrypted data (cipher text).

IV. RESULTS AND DISCUSSION

Through the Simulation, we can conclude that the time cost of our scheme is much smaller with
Figure 2: Efficiency comparison for different simulation times.
Different simulation times. In addition, it is easily observed that the performance of our scheme is more stable and the second result that we come upon is that number of participant in our scheme can participate more and they can efficiently access the system without any errors. The result bar sows how the system raises up.

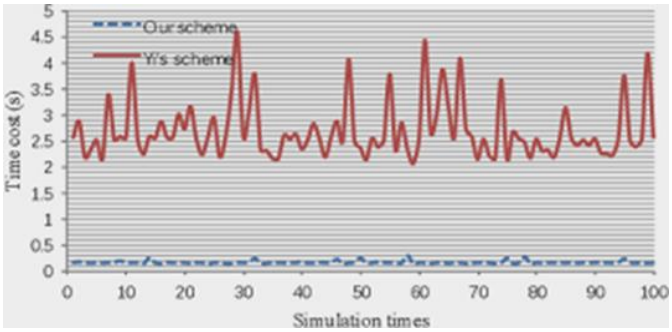

Figure 3: Efficiency comparison for multiple participants.

V. CONCLUSION

We present a unique block design-based key agreement protocol that supports cluster knowledge sharing in cloud computing. Multiple participants will be concerned within the protocol and general formulas of the common conference key for participation ar derived. Moreover, the introduction of volunteers allows the given protocol to support the fault tolerance property, thereby creating the protocol additional sensible and secure. In our future work, we might wish to extend our protocol to supply additional properties to form it applicable for a spread

of environments. As a development within the technology of the web and cryptography, cluster knowledge sharing in cloud computing has opened up a replacement space of quality to laptop networks. With the assistance of the conference key agreement protocol, the security and potency of cluster knowledge sharing in cloud computing is greatly improved. Specifically, the outsourced data of the information house owners encrypted by the common conference key square measure shielded from the attacks of adversaries. Compared with conference key distribution, the conference key agreement has qualities of upper safety and responsibility. However, the conference key agreement asks for an outsized amount of knowledge interaction within the system and a lot of computational price. To combat the issues within the conference key agreement, the SBIBD is used within the protocol design. Results and discussion may be combined into a common section or obtainable separately. They may also be broken into subsets with short, revealing captions. An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it. This section should be typed in character size 10pt Times New Roman.

VI. REFERENCES

[1]. 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.

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

[3]. L. Zhou, V. Varadharajan, and M. Hitchens, “Cryptographic rolebasedaccess control for secure cloud data storage systems,” InformationForensics and Security IEEE Transactions on, vol. 10, no. 11,pp. 2381–2395, 2015.

Cite this article as :

Wajiha Nausheen, Shital Gaikwad, " Group Data Sharing in Cloud Computing with Secure Key Agreement Modal", International Journal of Scientific Research in Science and Technology(IJSRST), Print ISSN : 2395-6011, Online ISSN : 2395-602X, Volume 8, Issue 4, pp.500-504, July-August-2021. Available at Journal URL : https://ijsrst.com/IJSRST218473