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

Ajinkya Abhay Shinde, Yogesh Appaso Dhuke, Avishkar Vitthal Wagh, Prof. S. B. Bandgar
Computer Engineering ,SB Patil College of Engineering, Indapur Pune

Abstract: Data sharing in cloud computing permits multiple participants to freely share the cluster knowledge that improves the efficiency of labor in cooperative environments and has widespread potential applications. However, some way to form sure the safety of information sharing among and therefore the thanks to with efficiency share the out sourced information in Associate in Nursing extremely cluster manner area unit formidable challenges. Note that key agreement protocols have contend a really necessary role in secure and economical cluster knowledge sharing in cloud computing. During this paper, by taking advantage of the Centro symmetric balanced incomplete block vogue (SBIBD), we tend to gift a unique block design-based key agreement protocol that supports multiple participants, which can exile extend the number of participants in Associate in Nursing extremely cloud surroundings the structure of the block style. Supported the planned cluster knowledge sharing model, we've a bent to gift general formulas for generating the common conference key K for multiple participants. Note that by taking advantage of the block style, the process complexness of the planned protocol linearly can increase with the number of participants and additionally the communication quality is greatly reduced. To boot, the fault tolerance property of our protocol permits the cluster knowledge sharing in cloud computing to face up to different key attacks, that's analogous to protocol.

Keywords :Key agreement protocol, centro symmetric balanced incomplete block style (SBIBD), data sharing, cloud computing.

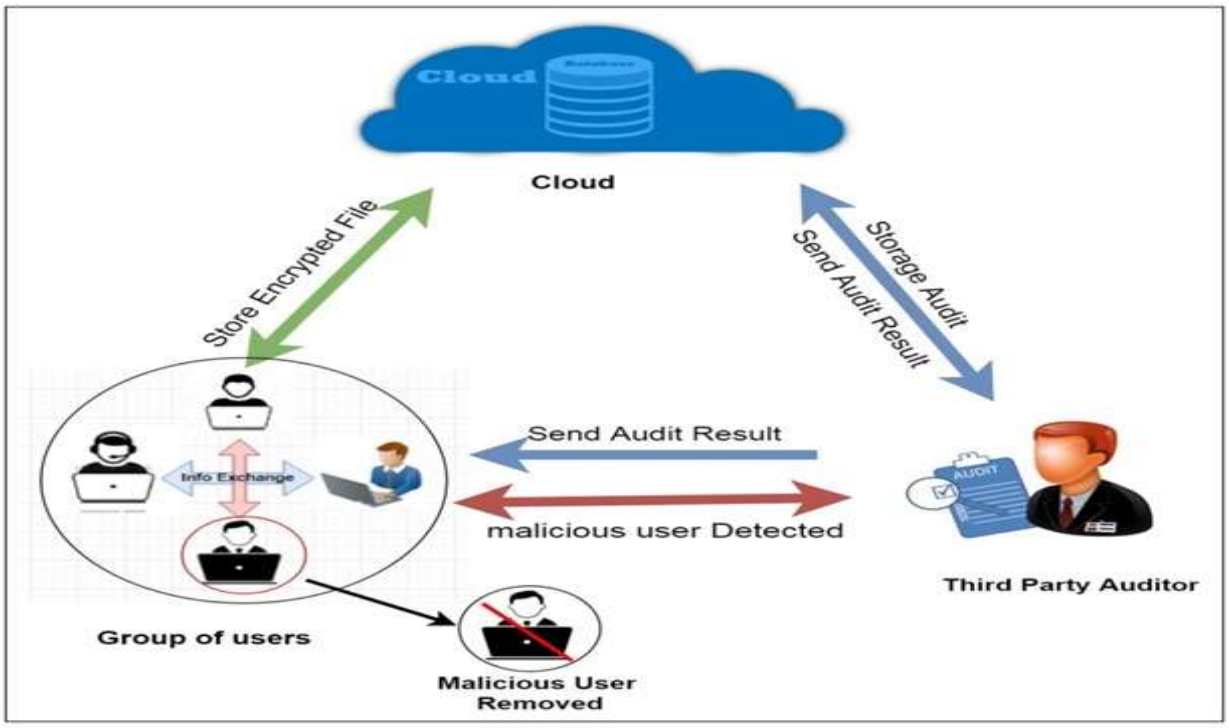
Introduction: CLOUD computing and cloud storage have become hot topics in recent decades. Area unit ever-changing the approach we have a tendency to live and greatly rising production potency in some areas. At present, thanks to restricted storage resources and also the requirement for convenient access, we have a tendency to like better to store all types of information in cloud servers, that is additionally an honest possibility for corporations and organizations to avoid the overhead of deploying and maintaining instrumentality once information area unit keep locally. The cloud server provides associate degree open and convenient storage platform for people and organizations, but it also introduces security issues. as an example, a cloud system could also be subjected to attacks from each malicious users and cloud suppliers. In these eventualities, it's vital to ensure the protection of the keep information within the cloud. In many schemes were planned to preserve the privacy of the outsourced information. The higher than schemes solely considered security issues of one information owner. However, in some applications, multiple information house owners would really like to firmly share their information during a cluster manner. Therefore, a protocol that supports secure cluster information sharing underneath cloud computing is required. A key agreement protocol is employed to get a standard conference key for multiple participants to make sure the protection of their later communications, and this protocol is applied in cloud computing to support secure and economical data sharing. Since it absolutely was introduced by Diffie-Hellman in their seminal paper, the key agreement protocol has become one among the basic crypto logical primitives. The basic version of the Diffie-Hellman protocol provides associate degree efficient answer to the matter of making a standard secret key between 2 participants. In cryptography, a key agreement protocol could be a protocol within which 2 or additional parties can agree on a key in such the way that each influence the result. By using the key agreement protocol, the conferees can 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 individual cannot get the

generated key by implementing malicious attacks, like eavesdropping. Thus, the key agreement protocol is wide utilized in interactive communication environments with high security requirements (e.g., remote board conferences, teleconferences, collaborative workspaces, oftenest identification cloud computing so on). The Diffie-Hellman key agreement provides the way to generate keys. However, it doesn't give associate degree authentication service, that makes it at risk of man in the middle attacks. This example is addressed by adding some types of authentication mechanisms to the protocol, as planned by Law et al. in. additionally, the Diffie-Hellman key agreement will solely support 2 participants. afterwards, to resolve the various key attacks

Problem Statement:

In block design based key agreement protocol system, we proposed a block design based key agreement protocol that supports multiple participants, which can flexibly extend the number of participants. Generate a common group key K for multiple participants to share securely data in group. Existing system operate only when all group participant are honest, but do not work when some group members are malicious and attempt to delay or destruct the group.

Architecture Diagram:



Mathematical Model:

Input:

Large Bandwidth Network, movable device, sensor

Output:

Successful communication between two devices

System Description

1. Input: Set of outsourced data sets by corresponding data user.
2. Output: Securely data sharing with group participant and remove malicious user from group through TPA.
3. System Used:

1. TPA for auditing on data and remove malecious users

Let S is the system, S= I, P, O,IS,OS,F,G,f1,f2

Where,I-Input,

P- procedure,

O- Output.

I-F,G

F- data les set of f1,f2,,fn

G- Group Users Query g1,g2,,qN

Procedure(P):
Where :
TPA=Third Party Auditor,
F=FaultTolerance
B=Set of block.
V=No of group participant.
ei = PublicKey
di = PrivateKey
H1,h2=HashFunction
Identify failure cases as F
F=fshare data to malicious user in group.g
Identify success as s.
s=share data in group and give private key to all group participant and re-
move
malicious user from group.

Literature Survey:

1)Paper Name: Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data
Author: Ning Cao, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou
Description: With the advent of cloud computing, data owners are motivated to outsource their complex data management systems from local sites to the commercial public cloud for great flexibility and economic savings. But for protecting data privacy, sensitive data has to be encrypted before outsourcing, which obsoletes traditional data utilization based on plaintext keyword search. Thus, enabling an encrypted cloud data search service is of paramount importance. Considering the large number of data users and documents in the cloud, it is necessary to allow multiple keywords in the search request and return documents in the order of their relevance to these keywords. Related works on searchable encryption focus on single keyword search or Boolean keyword search, and rarely sort the search results. In this paper, for the first time, we define and solve the challenging problem of privacy preserving multi-keyword ranked search over encrypted cloud data (MRSE). We establish a set of strict privacy requirements for such a secure cloud data utilization system.

2) Paper Name: Enabling Cloud Storage Auditing with Key-Exposure Resistance
Author: Jia Yu, Kui Ren, Cong Wang
Description: Cloud storage auditing is viewed as an important service to verify the integrity of the data in public cloud. Current auditing protocols are all based on the assumption that the clients secret key for auditing is absolutely secure. However, such assumption may not always be held, due to the possibly weak sense of security and/or low security settings at the client. If such a secret key for auditing is exposed, most of the current auditing protocols would inevitably become unable to work. In this paper, we focus on this new aspect of cloud storage auditing. We investigate how to reduce the damage of the clients key exposure in cloud storage auditing, and give the first practical solution for this new problem setting. We formalize the definition and the security model of auditing protocol with key-exposure resilience and propose such a protocol. In our design, we employ the binary tree structure and the pre-order traversal technique to update the secret keys for the client. We also develop a novel authenticator construction to support the forward security and the property of block less very ability. The security proof and the performance analysis show that our proposed protocol is secure and efficient.

3) Paper Name: Enabling Cloud Storage Auditing With Verifiable Outsourcing of Key Updates
Author: Jia Yu, Kui Ren and Cong Wang
Description: Key-exposure resistance has always been an important issue for in-depth cyber defence in many security applications. Recently, how to deal with the key exposure problem in the settings of cloud storage auditing has been proposed and studied. To address the challenge, existing solutions all require the client to update his secret keys in every time period, which may inevitably bring in new local burdens to the client, especially those with limited computation resources, such as mobile phones. In this paper, we focus on how to make the key updates as transparent as possible for the client and propose a new paradigm called cloud storage auditing with verifiable outsourcing of key updates. In this paradigm, key updates can be safely outsourced to some authorized party, and thus the key-update burden on the client will be kept minimal. In particular, we leverage the third party auditor (TPA) in many existing public auditing designs, let it play the role of authorized party in our case, and make it in charge of both the storage auditing and the secure key updates for key-exposure resistance.

4) Paper Name: Cryptanalysis of simple three-party key exchange protocol
Author Name: N.W. Lo, Kuo-Hui Yeh and Meng-Chih Chiang
Description: Three-party authenticated key exchange (3PAKE) protocol plays an indispensable role in history of the secure communication areas in which two clients can agree a robust session key based on a human-memorable password. Current research community focuses on the issue of designing a simple 3PAKE (S-3PAKE) protocol which possesses both of robust system security and efficient computation complexity. In 2008, Chung and Ku pointed out that Lu and Caos S3PAKE scheme cannot resist three variants of the man- in-themiddle attack. The authors proposed a countermeasure to eliminate the identified weaknesses. Nevertheless, based on our security analysis, the S-3PAKE mechanism proposed by Chung and Ku is vulnerable to the undetectable on-line dictionary attack. In this paper, we review Chung and Kus S-3PAKE protocol and analyze its robustness. For security enhancement, a modified S-3PAKE scheme is introduced to resist to the undetectable on-line dictionary attack

5) Paper Name: Provably authenticated group diffe-hellman key exchange
Author Name: H. Guo, Z. Li
Description: Group Diffe-Hellman protocols for Authenticated Key Exchange (AKE) are designed to provide a pool of players with a shared secret key which may later be used, for example, to achieve multicast message integrity. Over the years, several schemes have been o ered. However, no formal treatment for this cryptographic problem has ever been suggested. this paper, we present a security model for this problem and use it to precisely define AKE (with implicit authentication) as the fundamental goal, and the entity- authentication goal as well. We then define in this model the execution of an authenticated group Diffe-Hellman scheme and prove its security.

Contribution : In this paper, 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. The main contributions of this paper are summarized as follows.
1. Model of group data sharing according to the structure of the SBIBD is constructed. In this paper, a group data sharing model is established based on the definition of the SBIBD, which can be used to determine the way of communication among the participants. Regarding mathematical descriptions of the structure of the SBIBD, general formulas for computing the common conference key for multiple participants are derived.
2. Fault detection and fault tolerance can be provided in the protocol. The presented protocol can perform fault detection to ensure that a common conference key is established among all participants without failure. Moreover, in the fault detection phase, a volunteer will be used to replace a malicious participant to support the fault tolerance property.
The volunteer enables the protocol to resist different key attacks [7], which makes the group data sharing in cloud computing more secure.

Conclusion:
As a development within the technology of the web and cryptography, cluster knowledge sharing in cloud computing has opened up a brand new 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 will be greatly improved. Specifically, the outsourced data of the knowledge the info the information homeowners 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 dependableness. However, the conference key agreement asks for an oversized amount of knowledge interaction within the system and additional computational value. To combat the issues within the conference key agreement, the SBIBD is used within the protocol design. In this paper, we have a tendency to gift a completely unique block design-based key agreement protocol that supports cluster knowledge sharing in cloud computing. because of the definition and also the mathematical descriptions of the structure of a (v; k + 1; 1)-

design, multiple participants will be concerned within the protocol and general formulas of the common conference key for participate in square measure derived. Moreover, the introduction of volunteers permits the bestowed protocol to support the fault tolerance property, thereby creating the protocol additional practical and secure. In our future work, we might like to extend our protocol to produce additional properties (e.g., anonymity, traceability, and then on) to create it applicable for a variety of environments.

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] 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.
[3] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976.
[4] 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.
[5] 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.
[6] X. Yi, "Identity-based fault-tolerant conference key agreement," IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 3, pp. 170–178, 2004.
[7] 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.
[8] 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.
[9] B. Dan and M. Franklin, "Identity-based encryption from the well pairing," Siam Journal on Computing, vol. 32, no. 3, pp. 213–229, 2003.
[10] S. Blakewilson, D. Johnson, and A. Menezes, "Key agreement protocols and their security analysis," in IMA International Conference on Cryptography and Coding, 1997, pp. 30–45.