Secure Key Agreement Model for Group Data Sharing in Cloud Computing

Khilesh Rama Barela[1] Sameer GovindWagh[2] Vishal RajaramWalunj[3] MadanTukaramKutke[4] Prof. Priyanka R. Naoghare[5]

[1,2,3,4,5]Loknete Gopinathji Munde Institute of Engineering Education & Research

Abstract— Data sharing in cloud computing allows multiple participants to freely share the group data, that improves the potency of work in cooperative environments and has widespread potential applications. However, a way to make sure the security of data sharing within and the way to with efficiency share the outsourced knowledge in an exceedingly group manner square measure formidable challenges. Note that key agreement protocols have compete a really necessary role in secure and economical group data sharing in cloud computing. In this paper, by taking advantage of the symmetric balanced incomplete block style (SBIBD), we present a novel block design-based key agreement protocol that supports multiple participants, which may flexibly extend the quantity of participants in an exceedingly cloud surroundings the structure of the block design. supported the planned group data sharing model,

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 is analogous to Yi's protocol.

Key words: Group Data Sharing, Cloud Computing

I. INTRODUCTION

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 can not 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.

Fault detection and fault tolerance is provided within the protocol. The conferred protocol will perform

fault detection to confirm that a typical conference secret's established among all participants while not failure. Moreover, within the fault detection part, a volunteer are won't to replace a malicious participant to support the fault tolerance property. The volunteer allows the protocol to resist completely different key attacks that makes the cluster information sharing in cloud computing safer. 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.

II. RELATED WORK

A. Cryptanalysis of simple three-party key exchange protocol.

we show that this protocol is vulnerable to a kind of man-in-the-middle attack that exploits an authentication flaw in their protocol and is subject to the undetectable on-line dictionary attack. We also conduct a detailed analysis on the flaws in the protocol and provide an improved protocol. We have analyzed the security of simple three-party protocol for password-authenticated key exchanges. Although Lu and Cao claimed their protocol can resist against various known attacks, we have shown that the protocol is indeed completely insecure against a kind of man-in-the-middle attack and the undetectable on-line dictionary attack. In addition, we have provided an improved protocol that addresses the identified security problems.

B. Enabling Storage Auditing In Cloud of Key Updates from Verifiable Outsource.

In this project, the study on how to outsource key updates for cloud storage auditing through key exposure resilience. It propose the first cloud storage auditing protocol by verifiable outsourcing of key updates. In this protocol, key updates are out sourced to the TPA and are transparent for the client. In addition, the TPA only sees the encrypted version of the client's secret key, as the client can further verify the validity of the encrypted secret keys when downloading them from the TPA. That offer the formal security proof and the performance simulation of the proposed schemeEnabling Cloud Storage Auditing with Key Exposure Resistance

It is investigated on how to reduce the damage of the client's key revelation in cloud storage auditing, and provide the first handy elucidation for this new problem setting. Formalized the definition and the security model of auditing protocol with key-exposure resilience and propose such a protocol. Utilized and developed a novel authenticator construction to support the forward security and the property of block less verifiability using the current design. The security proof and the performance analysis show that the projected protocol is protected and well-organized

C. Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data

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. Among various multi keyword semantics, we choose the efficient similarity measure of "coordinate matching", i.e., as many matches as possible, to capture the relevance of data documents to the search query. We further use "inner product similarity" to quantitatively evaluate such similarity measure. We first propose a basic idea for the MRSE based on secure inner product computation, and then give two significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given. Experiments on the real-world dataset further show proposed schemes indeed introduce low overhead on computation and communication.

D. Provably Authenticated Group Diffie-Hellman Key Exchange

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. Among various multi keyword semantics, we choose the efficient similarity measure of "coordinate matching", i.e., as many matches as possible, to capture the relevance of data documents to the search query. We further use "inner product similarity" to quantitatively evaluate such similarity measure. We first propose a basic idea for the MRSE based on secure inner product computation, and then give two significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given. Experiments on the real-world dataset further show proposed schemes indeed introduce low overhead on computation and communication.

We provide an exact analysis of thesecurity of the schemes rather than asymptotic ones. That is, we explicitly quantify the reduction from the security of ascheme to the security of the underlying "hard" problem(s)on which it is based. This allows us to know exactly howmuch security is maintained by the reduction and thus todetermine the strength of the reduction.This paper provides major contributions to the solutionof the group Diffie-Hellman key exchange problem. We firstpresent a formal model to help manage the complexity ofdefinitions and proofs for the authenticated group Diffie-Hellman key exchange. A model where a process controlledby a player running on some machine is modeled as an instanceof the player, the various types of attacks are modelled by queries to these instances and the security of the sessionkey is modeled through semantic security. Moreover, inorder to be correctly formalized, the intuition behind mutual authentication needs cumbersome definitions of session IDS and partner IDS which can be skipped at the primary. They argued that their

easy many-sided PAKE (3-PAKE) protocol will resist against varied noted attacks. during this paper, we have a tendency to show that this protocol is at risk of a form of man-in-the-middle attack that exploits associate authentication flaw in their protocol and is subject to the undetectable on-line wordbook attack. we have a tendency to additionally conduct a close associate analysis on the issues within the protocol and supply an improved protocol. Existing auditing protocols square measure all supported the supposition that the Client's secret key for auditing is totally protected. Such assumption might not continually be command, as a result of the most likely weak sense of security and/or low security settings at the shopper. In most of this auditing protocols would inevitably become unable to figure once a secret key for auditing is exposed. we propose two specific secure cloud storage protocols based on two recent secure network coding protocols. In particular, we obtain the first publicly verifiable secure cloud storage protocol in the standard model. We also enhance the proposed generic construction to support user anonymity and third-party public auditing, which both have received considerable attention recently. Finally, we prototype the newly proposed protocol and evaluate its performance. Experimental results validate the effectiveness of the protocol.

III. EXISTING SYSTEM

In Existing System variant conference key agreement protocols square measure steered to secure system conference. Most of them operate as long as all conferees unit of measurement honest, but do not work once some conferees unit of measurement malicious and attempt to delay or destruct the conference. Recently, Tzeng planned a conference key agreement protocol with fault tolerance in terms that a typical secret conference key among honest conferees could also be established yet malicious conferees exist. among the case where a conferee can broadcast fully totally different messages in varied sub networks, Tzeng's protocol is liable to a "different key attack" from malicious conferees.

A. Disadvantages

1) Existing schemes have some disadvantage, it is used when Most of them operate only when all group members are honest.
2) Do not work when some group members are malicious and attempt to delay or destruct the conference.

IV. PROPOSE SYSTEM

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.

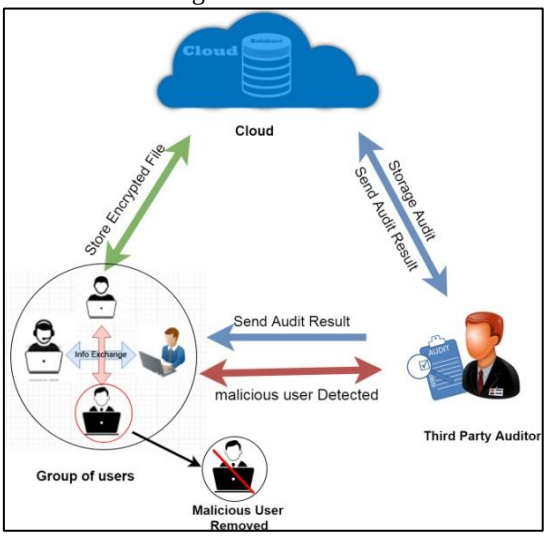

Fig. 1: System Architecture

A. 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.

B. Mathematical Model

1) LetSbeasystem.S={I,O,P,F,s,Ic}
2) IdentifysetofinputasI
   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, e_i , d_i ,H1,H2 }
   TPA=ThirdPartyAuditor.
   B=Set of block.
   V=No of group participant.
   K=.Key Agreement.
   F=FaultTolerance
   e_i= PublicKey
   d_i = 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={Outsourceddatawithitsprivacyprivilegestobemaintain)

V. ALGORITHM

A. RSA Algorithm:

RSA is algorithm used by modern Computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone. The other key must be kept private. It is based on the fact that finding the factors of an integer is hard.

B. Steps of RSA Algorithm:

1) Step 1 – Choose two prime numbers, Prime1 and Prime2 to get the product Of Prime1 Prime2 variable.
2) Step 2 – Find the Totient of Product Of Prime1 Prime2.
   Totient uses a weird symbol that looks like the letter 'p' but is not.
3) Step 3 – Get a list of possible integers that result in 1 mod Totient
4) Step 5 – Choose a 1 mod Totient value with exactly two prime factors: Encrypt Prime and Decrypt Prime
5) Step 6 – Encrypt
   We now have everything we need to Encrypt and Decrypt.
6) Step 6 – Decrypt

VI. 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.

REFERENCES

[1] 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.
[2] F. Chen, T. Xiang, Y. Yang, and S. S. M. Chow, "Secure cloudstorage meets with secure network coding," in IEEE INFOCOM,2014, pp. 673–681.
[3] D. He, S. Zeadally, and L.Wu, "Certificateless public auditingscheme for cloud-assisted wireless body area networks," IEEESystems 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 rfidauthentication 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, "Anefficient protocol for authenticated key agreement," Designs Codesand 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 tomulti party key agreement (extended abstract)." Lecture Notes inComputer Science, vol. 2003, pp. 205–217, 2003.
[9] J. Shen, S. Moh, and I. Chung, "Identity-based key agreement protocolemploying 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 weilpairing," Siam Journal on Computing, vol. 32, no. 3, pp. 213–229,2003.
[11] S. Blakewilson, D. Johnson, and A. Menezes, "Key agreement protocolsand their security analysis," in IMA International Conferenceon Cryptography and Coding, 1997, pp. 30–45.
[12] I. Chung and Y. Bae, "The design of an efficient load balancingalgorithm employing block design," Journal of Applied Mathematicsand Computing, vol. 14, no. 1, pp. 343–351, 2004.
[13] O. Lee, S. Yoo, B. Park, and I. Chung, "The design and analysisof an efficient load balancing algorithm employing the symmetricbalanced incomplete block design." Information Sciences, vol. 176,no. 15, pp. 2148–2160, 2006.
[14] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchablesymmetric encryption: Improved definitions and efficient constructions,"Journal of Computer Security, vol. 19, no. 5, pp. 79–88, 2011.

