International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017), e-ISSN: 2455-2585
Volume 5, Issue 5, May-2019

Enhancing Efficiency and Security for Group Information Sharing using Key Agreement protocol in Cloud Computing

Avishkar Suryavanshi, Pratibha Kushire, Onkar Solat, Snehal Somuse, Prof.Shyam Gupta

Computer Department, Siddhant College of Engineering

Abstract: ***Data sharing in cloud computing permits multiple participants to freely share the group information thathelps in improving the efficiency of work in cooperative environments and has widespread potential applications.However, ensuring the security of information sharing within a group and outsourcing the group information efficiently is an alarming challenge. Note that key agreement protocols like RSA plays a crucial rolein securing group information sharing in cloud computing. In this paper, by taking the advantage of key agreement algorithms and by setting the threshold percentage of key for accessing the data we are designing a secure and efficient group information sharing system. By using auditing the malicious user is also detected by the system. In addition, the fault tolerance property of our system enables the group information sharing in cloud computing to withstand key attacks like giving wrong key by the group member.***

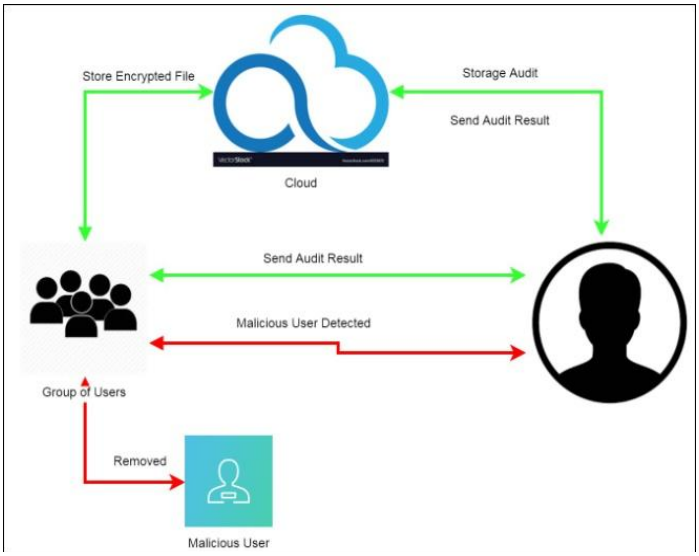
Keywords: Key agreement protocol, encryption, decryption, data sharing, cloud computing, security, auditing.

INTRODUCTION

CLOUD computing and cloudstorage became hot topics in recent decades. At present, owing to restricted storageresources and besides the requirement for convenientaccess, we've associate inclination to love higher tostore all types of info in cloud servers,that is besides associate honest chance forcorporations and organizations to avoid theoverhead of deploying and maintaininginstrumentality once info unit keepregionally. The cloud server provides degree open and convenient storage platform for people andorganizations, however it besides introduces securityissues.

As associate example, a cloud system could evenbe subjected to attacks from every malicious usersand cloud suppliers. In these eventualities, it's very important to substantiate the protection of thekeep info among the cloud. In manyschemes were planned to pre serve the privacy of the outsourced info. The upper thanschemes alone thought-about security problems withone info owner. However, in someapplications, multiple info householderswould like to firmly share their infothroughout a cluster manner. Therefore, a protocolthat supports secure cluster info sharingbelow cloud computing is needed. A keyagreement protocol is utilized to urge a dailyconference key for multiple participants to createbound the protection of their latercommunications,and this protocol is applied incloud computing to support secure andeconomical info sharing. Since it totally wasintroduced by Diffie-Hellman in their seminalpaper, the key agreement protocol has become oneamong the essential crypto logical primitives. The essential version of the Diffie-Hellman protocolprovides degree economical answer to the matterof constructing a daily secret key between a strive ofparticipants. In cryptography, a key agreementprotocol could be a protocol among that a striveof or any parties will agree on a key in such thestrategy that every influence the result. By observethe key agreement protocol, the conferees will firmly send and receive messages from oneanother observe the common conference key thatthey agree upon beforehand. Specifically, a securekey agreement protocol ensures that the individualcannot get the generated key by implementingmalicious attacks, like eavesdropping. Thus, thekey agreement protocol is wide utilised ininteractive communication environments withhigh security desires (e.g., remote board conferences, teleconferences, cooperative workspaces, oftenest identification cloud computing thus on). The Diffie-Hellman keyagreement provides the owing to generate keys. However, it does not offer degree authentication service that produces it in peril of man among thecenter attacks. this instance is addressed byadding some types of authentication mechanismsto the protocol, as planned by Law et al. in. toboot, the Diffie-Hellman key agreement cansolely support a strive of participants. Afterwards, toresolve the varied key attacks.

ARCHITECTURE DIAGRAM



MATHEMATICAL MODEL

System:S={I,P,O }where S=SystemI=InputP=ProcedureO=Output

Input: I={GrpUsr,pk,sk,F,mls_U,dvalue,EncFile,DecFile}

Where GrpUsr=Group user/group Memberpk=Public keysk=Secret KeyF=Number of files f1,f2,f3,….fnmls=malicious User dvalue=Digest ValueEncFile= Encryption File DecFile=Decryption File

Procedure:p= { EncryptFile,File,pk,GrpUser,verifyFile,dvalu,skm,grpkey,decrFile,grpk,mlcsUser}

Where, Encrypt File=Encrypted Filepk= Public key for Encryption GrpUser=Group Member or Group UsersverifyFile=Veriufy Cloud file using TPAdvalue=Digest Value/Hash Value for Data verifysk=Secret key for Data download in Decryption Formatgrpkey=Group Member Authentication KeydecrFile=Decryption KeymlcsUser= Malicious User

Step 1: Upload File in groupEncryptFile=Upload(File,pk)<-GrpUser

Step 2: Verify File from TPAverifyFile=(EncrFile,dvalue)

Step 3: Access The File Group memberGrpUser=F(EncryptFile,Sk)

Step 4: Request SK to Group User sk=(u1,u2,u3,….,un)

Step 5: Access the File using skdecrFile=F(EncrFile,Sk,Grpkey)

Step 6: File Download in Decryptiondownload=(decrFile,Sk)

Step 7: Detect malicious UsermlcsUser=(gmk1,gmk2,..grpkworng….grpkn)

Step 8: Remove Malicious User

Output:O =1) Files Securely Share in Group in Encryption format.

2) Also, verify file from TPA using dvalue

3) Data User download the file based on threshold authentication in Decryption format

4) TPA detect the Malicious User with MAC Address

LITERATURE SURVEY

1)Paper Name: Privacy-Preserving Multikeyword 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 plaintextkeyword search. Thus, enabling an encryptedcloud data search service is of paramountimportance. Considering the large number of datausers and documents in the cloud, it is necessaryto allow multiple keywords in the search request and return documents in the order of theirrelevance to these keywords. Related works onsearchable encryption focus on single keywordsearch or Boolean keyword search, and rarely sortthe search results. In this system, for the first time,we define and solve the challenging problem ofprivacy preserving multi-keyword ranked searchover encrypted cloud data (MRSE). We establisha set of strict privacy requirements for such asecure cloud data utilization system.

2) Paper Name: Enabling Cloud StorageAuditing with Key-Exposure Resistance

Author: Jia Yu, Kui Ren, Cong Wang

Description: Cloud storage auditing is viewed 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 securityand/or low security settings at the client. If such asecret key for auditing is exposed, most of thecurrent auditing protocols would inevitablybecome unable to work. In this system, we focuson this new aspect of cloud storage auditing. Weinvestigate how to reduce the damage of theclients key exposure in cloud storage auditing, and give the first practical solution for this newproblem setting. We formalize the definition andthe security model of auditing protocol with keyexposureresilience and propose such a protocol.In our design, we employ the binary tree structureand the pre-order traversal technique to update thesecret keys for the client. We also develop a novelauthenticator construction to support the forwardsecurity and the property of block less veryability. The security proof and the performanceanalysis show that our proposed protocol is secureand efficient.

3) Paper Name: Enabling Cloud StorageAuditing With Verifiable Outsourcing of KeyUpdates

Author: Jia Yu, Kui Ren and Cong Wang

Description: Key-exposure resistance has alwaysbeen an important issue for in-depth cyberdefence in many security applications. Recently,how to deal with the key exposure problem in thesettings of cloud storage auditing has beenproposed and studied. To address the challenge, existing solutions all require the client to updatehis secret keys in every time period, which mayinevitably bring in new local burdens to the client,especially those with limited computationresources, such as mobile phones. In this system,we focus on how to make the key updates astransparent as possible for the client and propose anew paradigm called cloud storage auditing withverifiable outsourcing of key updates. In thisparadigm, key updates can be safely outsourced tosome authorized party, and thus the key-updateburden on the client will be kept minimal. Inparticular, we leverage the third party audit or(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 auditingand the secure key updates for key-exposureresistance.

4) Paper Name: Cryptanalysis of simple threepartykey exchange protocol

Author Name: N.W. Lo, Kuo-Hui Yeh and Meng-Chih Chiang

Description: Three-party authenticated keyexchange (3PAKE) protocol plays anindispensable role in history of the securecommunication areas in which two clients can agree a robust session key based on a humanmemorablepassword. Current research community focuses on the issue of designing a simple 3PAKE (S-3PAKE) protocol whichpossesses both of robust system security andefficient computation complexity. In 2008, Chungand Ku pointed out that Lu and Caos S3PAKEscheme cannot resist three variants of the man- in-the-middleattack.

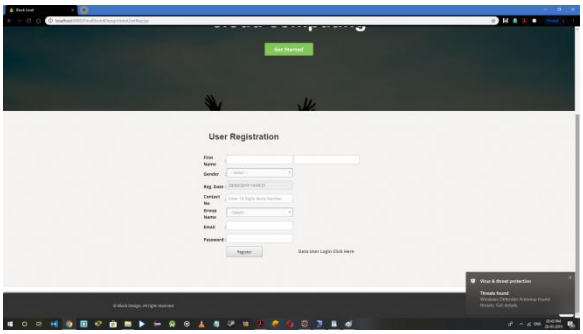
The authors proposed a countermeasure to eliminate the identifiedweaknesses. Nevertheless, based on our securityanalysis, the S-3PAKE mechanism proposed byChung and Ku is vulnerable to the undetectableon-line dictionary attack. In this system, wereview Chung and Kus S-3PAKE protocol andanalyze its robustness. For security enhancement, a modified S-3PAKE scheme is introduced toresist to the undetectable on-line dictionary attack

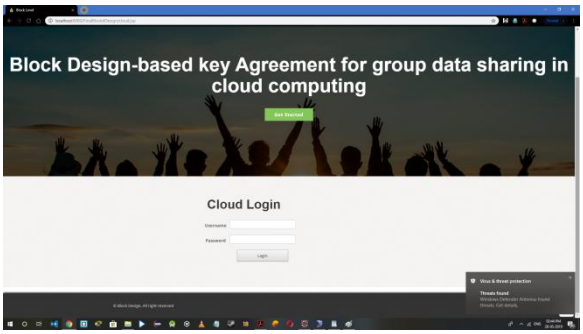
5) Paper Name: Provably authenticated group diffe-hellman key exchange

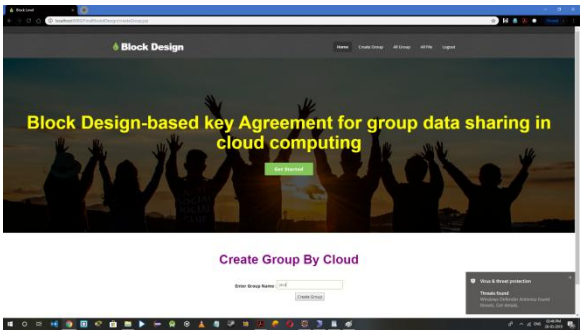
Author Name: H. Guo, Z. Li

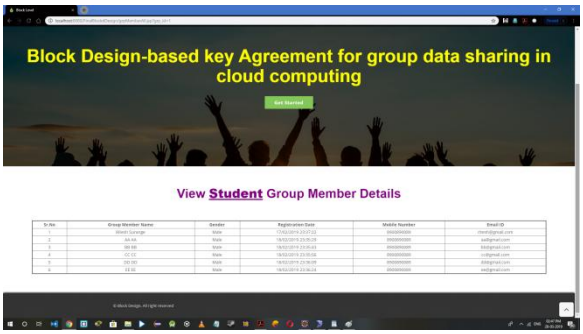
Description: Group Diffe-Hellman protocols forAuthenticated Key Exchange (AKE) are designedto provide a pool of players with a shared secretkey which may later be used, for example, toachieve multicast message integrity. Over theyears, several schemes have been offered. However, no formal treatment for thiscryptographic problem has ever been suggested.this paper, we present a security model for thisproblem and use it to precisely define AKE (withimplicit authentication) as the fundamental goal,and the entity- authentication goal as well. Wethen define in this model the execution of anauthenticated group Diffe-Hellman scheme andprove its security.

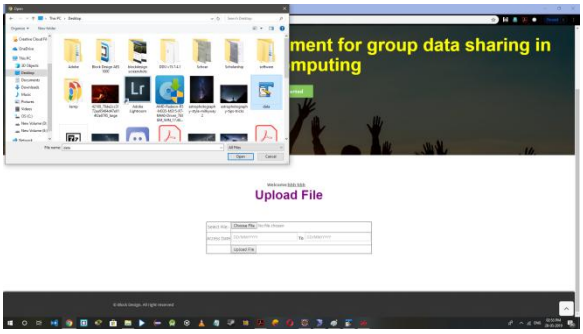
Screen shots:

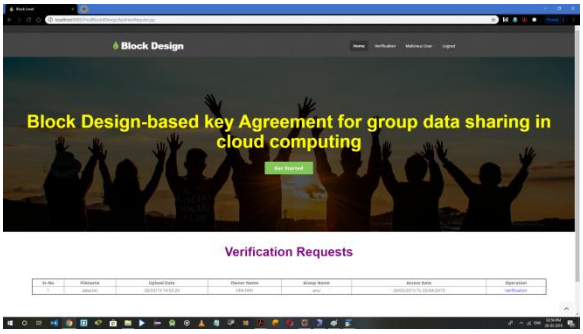












Contribution In this system, we tend to gift associate degreeefficient and secure block design-based keyagreement protocol by extending the structure ofthe SBIBD to support multiple participants, whichenables multiple knowledge homeowners to freely share theoutsourced knowledge with high security and potency.Note that the SBIBD is made because the clusterdata sharing model to support cluster knowledge sharingin cloud computing. Moreover, the protocol willprovide authentication services and a faulttolerance property. the most contributions of thispaper area unit summarized as follows.

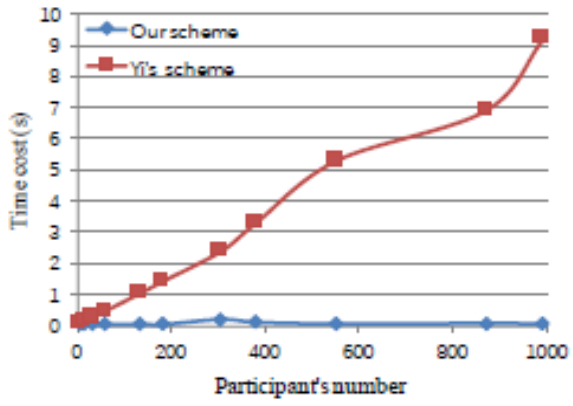
1. Model of cluster knowledge sharing consistent with thestructure of the SBIBD is made. In thissystem, a bunch knowledge sharing model is establishedbased on the definition of the SBIBD, which canbe wont to confirm the manner of communicationamong the participants. relating to mathematicaldescriptions of the structure of the SBIBD,general formulas for computing the commonconference key for multiple participants area unitderived.

2. Fault detection and fault tolerance may beprovided within the protocol. The conferred protocolcan perform fault detection to make sure that acommon conference key's established among allparticipants while not failure. Moreover, within the faultdetection section, a volunteer are wont toreplace a malicious participant to support the faulttolerance property.The volunteer permits the protocol to resistdifferent key attacks, that makes the cluster knowledgesharing in cloud computing safer.

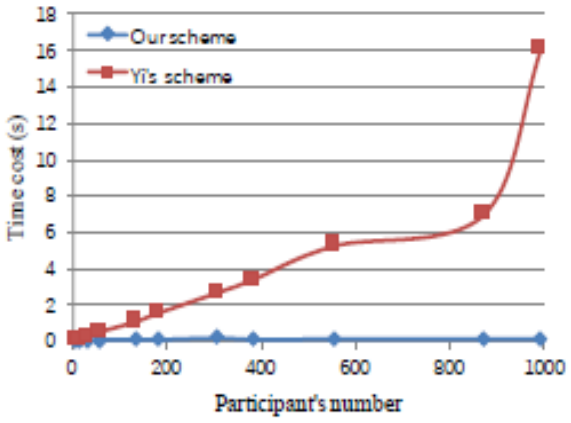
Problem Statement:

In block style primarily based key agreement protocolsystem, within the projected system a block stylebased key agreement protocol that supportsmultiple participants, which may flexibly extendthe number of participants. Generate a standardgroup key K for multiple participants to sharesecurely information in cluster. Existing system operateonly when all cluster participant are honest, but donot work once some cluster members are malicious and plan to delay or destruct thegroup.

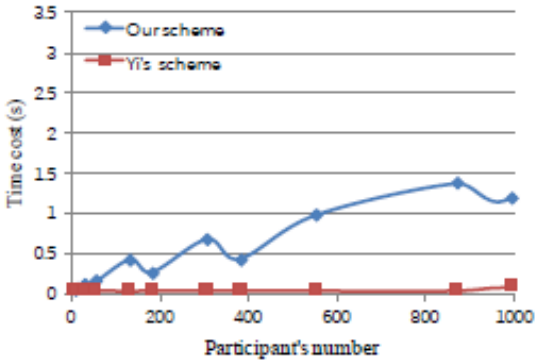
Efficiency comparison for different phases in Graphs



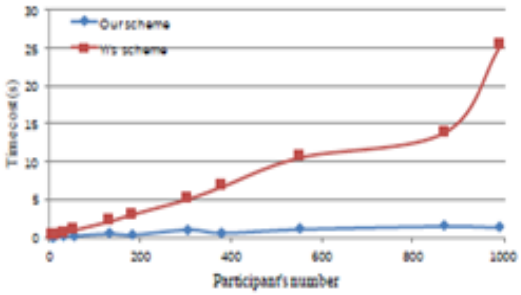
(a) Initial phase



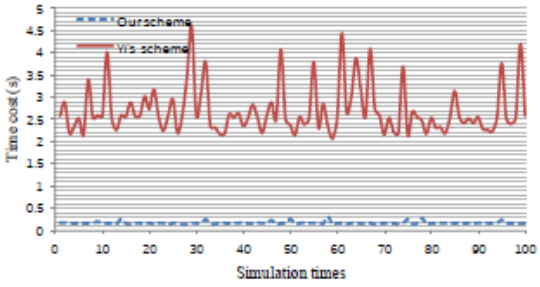
(b) Key agreement phase



(c) Authentication phase



Efficiency comparison for multiple participants.



Efficiency comparison for different simulation times.

Conclusion:

As a development among the technology of thenet and cryptography, cluster data sharing in cloud computing has detached a cub house ofquality to private pc networks. With theassistance of the conference key agreementprotocol, the protection and efficiency of clusterknowledge sharing in cloud computing have gottento be greatly improved. Specifically, theoutsourced knowledge of the data the information theknowledge householders encrypted by thecommon conference key unit protected against theattacks of adversaries. Compared with conferencekey distribution, the conference key agreementhas qualities of higher safety and accountable cape.However, the conference key agreement asks forAssociate in Nursing outsize quantity of knowledgeinteraction among the system and extramethod worth. To combat the problems among theconference key agreement, the SBIBD is employedamong the protocol vogue. throughout this paper,we have got Associate in Nursing inclination togift a very distinctive block design-basedkey agreement protocol that supports clusterknowledge sharing in cloud computing. Because of the definition and in addition the mathematicaldescriptions of the structure of a (v; k + 1; 1)- vogue, multiple participants have gotten to be concerned among the protocol and generalformulas of the common conference key forparticipate in unit derived. Moreover, theintroduction of volunteers permits the givenprotocol to support the fault tolerance property, thereby making the protocol a lot of sensible andsecure. In our future work, we'd wish to extendour protocol to provide a lot of properties (e.g.,anonymity, traceability, then on) to form itapplicable for a spread of environments.

References:

[1] F. Chen, T. Xiang, Y. Yang, and S. S. M. Chow, "Secure cloud storage meets with securenetwork 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 directionsin cryptography," IEEE Transactions onInformation 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 protocolproviding strong privacy and security," Journal ofInternet Technology, vol. 17, no. 3, p. 2, 2016.

[5] L. Law, A. Menezes, M. Qu, J. Solinas, and S.Vanstone, "An efficient protocol for authenticatedkey agreement," Designs Codes andCryptography, vol. 28, no. 2, pp. 119–134, 2010.

[6] X. Yi, "Identity-based fault-tolerantconference key agreement," IEEE Transactions onDependable and Secure Computing, vol. 1, no. 3,pp. 170–178, 2004.

[7] R. Barua, R. Dutta, and P. Sarkar, "Extendingjoux's protocol to multi party key agreement(extended abstract)." Lecture Notes in ComputerScience, vol. 2003, pp. 205–217, 2003.

[8] J. Shen, S. Moh, and I. Chung, "Identity-basedkey agreement protocol employing a symmetricbalanced incomplete block design," Journal ofCommunications and Networks, vol. 14, no. 6, pp.682–691, 2012.

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

[10] S. Blakewilson, D. Johnson, and A. Menezes,"Key agreement protocols and their securityanalysis," in IMA International Conference onCryptography and Coding, 1997, pp. 30–45.