Dual -Server PublicKey Encryption with Keyword SearchforSecure Cloud Storage

JHANSIDE VIRENA MALA
PGResearchScholar
S.R Engineeringcollege
Warangal,Telangana,India
JhansiDevi710@gmail.com

SYED NAWAZ PASHA
Assistant Professor in CSE
S.R Engineering college
Warangal,Telangana,India.
snp786@gmail.com

ABSTRACT: Cloud computing (CC) is a prototypical for assistingubiquitous network access to a remote server hosted over theinternet under a configurable computing resource. The control of this systems in the expanse of IT sector influences thestorage, online processing, data concept of network and software, etc. Since these services were compelling on the sharedmedium, the security needs to be enabled and maintained at the higher level.To address this security vulnerability, we propose another PEKS structure named Dual-ServerPublic Key Encryption with Keyword Search (DS-PEKS). As alternative fundamental obligation, we characterize another variation of theSmooth Projective Hash Functions (SPHFs) suggested to as straight and homomorphism SPHF (LH-SPHF). We then demonstrate abland development of secure DS-PEKS from LH-SPHF. To signify the possibility of our new structure, we give a proficientinstantiation of the general system from a DDH-based LH-SPHF and reveal that it can accomplish the solid security againstinside KGA.

KEYWORDS-Keyword search, secure cloud storage,encryption, inside keyword guessing attack.

I. INTRODUCTION

With the fast improvement of distributed computing and portable systems administration innovations,clients tend to get to their put away information from the remote distributed storage with cell phones. Thefundamental favorable position of distributed storage is its pervasive client availability furthermore its for all intentsand purposes boundless information stockpiling capacities. Notwithstanding such advantages gave by the cloud, thereal test that remaining parts is the worry over the secrecy and protection of information while embracing thedistributed storage administrations [1]. For example, decoded client information put away at the remote cloud servercan be defenseless against outer assaults started by unapproved outcasts and inside assaults started by the dishonestcloud service provider (CSPs) organizations [2]. There are a few reports that affirm information breaks identifiedwith cloud servers, because of malignant assault, burglary or inward mistakes [3]. This raises sympathy informationmay contain extremely delicate individual association/data.Distributed cloud storage outsourcing has turned into a prominent application for undertakings andassociations to lessen the weight of keeping up enormous information lately.No withstanding,in all actuality, end clients may not by any means believe the cloud capacity servers and may want to scramble theirinformation some time recently transferring them to the cloud server with a specific end goal to secure theinformation protection. This normally makes the information usage more troublesome than the conventional storagewhere information is kept in the nonappearance of encryption. One of the average arrangements is the searchableencryption which permits the client to recoverthe scrambled records that contain the client indicated catchphrases, where given the watchword trapdoor, the servercan discover the information required by the client without any problem .

The Problem is to determine how to securely search any document from cloud in form of encrypted data with the help of dual servers.

- Dual Server-public key encryption with keyword search (PEKS).
- How to Store data in Secure form on cloud.
- How to Store data in Secure form on cloud.

II. BACKGROUND WORKS

Cloud computing represents today's most exciting computing pattern shift in information technology[1]. but, security and privacy are perceived as primary obstacles to its large adoption[2]. Here, outline several criticalsecurity challenges and motivate further investigation of security solutions for a trustworthy public cloudenvironment[3]. cloud computing is the latest concept for the long-dreamed vision of computing as a usefulness. It isnecessary to store information on information storage servers such as mail servers and record servers in encodedframe to improve security and protection dangers. In any case, this typically suggests one needs to relinquishusefulness for security. For instance, if a customer wishes to recover just reports containing certain words, it was notbeforehand known how to let the information stockpiling server play out the inquiry and answer the questionwithout loss of information secrecy[4].the issue of seeking on information that is encoded utilizing an public open key framework. Consider clientBob who sends email to client Alice scrambled under Alice's open key. An email passage needs to test whether theemail contains the watchword \urgent" with the goal that it could course the email as needs be. Alice, then againdoes not wish to give the door the capacity to unscramble every one of her messages. We done and develop aninstrument that empowers Alice to give a key to the portal that empowers the door to test whether the word \urgent"is a watchword in the email without learning whatever else about the email. We allude to this system as Public KeyEncryption with watchword Search. As another case, consider a mail server that stores different messages openlyscrambled for Alice by others. Utilizing our instrument Alice can send the mail server a key that will empower theserver to distinguish all messages containing some keyword which is we want to search[5].

The decent property in this plan permits the server to scan for a catchphrase, given the trapdoor. Thus, the verifier can just utilize an untrusted server, which makes this idea extremely down to earth. Taking after Boneh etal's.work, there have been ensuing works that have been proposed to upgrade this idea. Two vital ideas incorporatethe supposed catchphrase speculating assault and secure channel free, proposed by Byun et al. what's more, Baek etal., separately. The previous understands the way that by and by, the space of the catchphrases utilized is extremelyconstrained, while the last considers the evacuation of secure channel between the beneficiary and the server tomake PEKS down to earth. Lamentably, the current development of PEKS secure against catchphrase speculatingassault is just secure under the irregular prophet display, which does not mirror its security in this present reality.Moreover, there is no total definition that catches secure channel free PEKS plans that are secure against pickedcatchphrase assault, picked ciphertextattack, and against watchword speculating assaults, despite the fact that thesethoughts appear to be the most pragmatic use of PEKS primitives[6].Aanother system, called secure server-assignment open key encryption with catchphrase seek (SPEKS),was acquainted with enhance the security of dPEKS (which experiences the on-line catchphrase speculating assault)by characterizing another security demonstrate 'unique ciphertextindistinguishability'[7].

III. PROPOSEDWORK

Tobegin with, in the preparatory work [1] where our nonspecific DS-PEKS development was exhibited, we indicatedneither a solid development of the straight what's more,homomorphism SPHF nor a reasonable instantiation of theDS-PEKS structure. To fill this crevice and outline theplausibility of the system, in this paper, we tobegin with demonstrate that a direct and homomorphismdialect LDH can be gotten from the Diffie-Hellmansupposition and at that point build a solid direct andhomomorphism SPHF, alluded to as $SPHF_{DH}$, from LDH.We give a formal verification that $SPHF_{DH}$ is right, smoothand pseudo-irregular development. We then present a solidDS-PEKS plot from $SPHF_{DH}$. To investigate its execution,we first give a correlation between existing plans and ourplan and after that assess its execution in trials. We tooreconsidered the preparatory adaptation [1] to upgrade thepresentation what's more, meaningfulness. In the relatedwork part, analyzed to the preparatory rendition, we includemore written works and give a clearer characterization of thecurrent plans in light of their security. We exhibit thesecurity models of DS-PESK as tests to make them morelucid. Besides, to make the ideas of SPHF and our recentlycharacterized vari clearer, we include Fig. 1and Fig. 2 tohighlight their key properties.

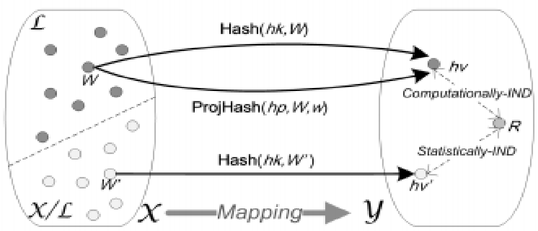

Fig. 1. Smooth projective hash function.

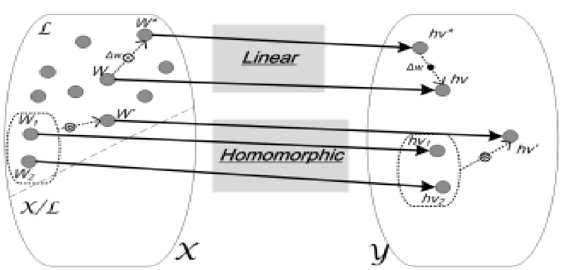

Fig. 2. Linear and Homomorphic SPHF.

A DS-PEKS plot primarily comprises of (KeyGen, DSPEKS, DS-Trapdoor; FrontTest; BackTest). To be moreexact, the KeyGen calculation creates general society/privatekey sets of the front and back servers rather than that of thecollector. Besides, the trapdoor era calculation DS-Trapdoorcharacterized here is open while in the customary PEKSdefinition [5], [13], the calculation Trapdoor takes as info

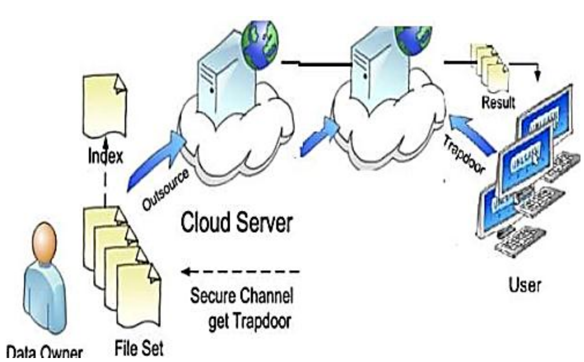

Fig .3 Dual server Architecture

Data Owner :Register with cloud server and login(username must be unique). Send request to Public key generator(PKG) to generate Key on the user name. Browse file and request Public key to encrypt the data, Upload data tocloud service provider. Verify the data from the cloud .

Public Key Generator :Receive request from the users to generate the key, Store all keys based on the user names. Check theusername and provide the private key. Revoke the end user (File Receiver if they try to hack file in the cloud serverand un revoke the user after updating the private key for the corresponding file based on the user).

Key Update :Receive all files from the data owner and store all files. Check the data integrity in the cloud and inform toend user about the data integrity. Send request to PKG to Update the private key of the user based on the dateparameter (Give some date to update Private Key). List all files, List all updated Private Key details based on thedate and users, List all File attackers and File Receive Attackers.

A. NEW FRAMEWORK FOR PEKS

In this segment, we formally define the Dual-Server PublicKey Encryption with Keyword Search (DS-PEKS) and itssecurity model.

Definition of DS-PEKS: A DS-PEKS scheme mainly consists of (KeyGen,DS − PEKS, DS − Trapdoor, FrontTest, BackTest). To bemore precise, the KeyGen algorithm generates the public/private key pairs of the front and back servers instead of thatof the receiver. Moreover, the trapdoor generation algorithmDS − Trapdoor defined here is public while in the traditionalPEKS definition [5], [13], the algorithm Trapdoor takes asinput the receiver’s private key. Such a difference is due to thedifferent structures used by the two systems. In the traditionalPEKS, since there is only one server, if the trapdoor generationalgorithm is public, then the server can launch a guessingattack against a keyword ciphertext to recover the encryptedkeyword. As a result, it is impossible to achieve the semanticsecurity as defined in [5] and [13]. However, as we will showlater, under the DS-PEKS framework, we can still achievesemantic security when the trapdoor generation algorithm ispublic. Another difference between the traditional PEKS andour proposed DS-PEKS is that the test algorithm is dividedinto two algorithms, FrontTest and BackTest run by twoindependent servers. This is essential for achieving securityagainst the inside keyword guessing attack.

In the DS-PEKS system, upon receiving a query from thereceiver, the front server pre-processes the trapdoor and all thePEKS ciphertexts using its private key, and then sends someinternal testing-states to the back server with the corresponding trapdoor and PEKS ciphertexts hidden. The back servercan then decide which documents are queried by the receiverusing its private key and the received internal testing-statesfrom the front server. The formal definition of DS-PEKS is asfollows.

Definition 1 (DS-PEKS): A DS-PEKS scheme is defined bythe following algorithms.

1)Setup(1): Takes as input the security parameter, generates the system parameters P;

2)KeyGen(P): Takes as input the systems parametersP,outputs the public/secret key pairs (pk_{FS}; sk_{FS}),and(pk_{BS}; sk_{BS}) for the front server, and the back serverrespectively;

3)DS-PEKS(P; pk_{FS}; pk_{BS}; kw1): Takes as input P, thefront server's public key pk_{FS}, the back server's publickey pk_{BS} and the keyword kw1, outputs the PE_{KS}ciphertext CT_{kw1} of kw1;

4) DS-Trapdoor(P; pkFS; pkBS; kw2): Takes as input P, thefront server's public key pkFS, the back server's publickey pkBS and the keyword kw2, outputs the trapdoorTkw2 ;

5) FrontTest(P; sk_{FS};CTkw1 ; Tkw2): Takes as input P,the front server's secret key sk_{FS}, the PE_{KS} ciphertextCT_{kw1} and the trapdoor T_{kw2} , outputs the internaltesting-state C_{ITS};

6)BackTest(P; sk_{BS};C_{ITS}): Takes as input P, the backserver's secret key sk_{BS} and the internal testing-stateC_{ITS}, outputs the testing result0 or 1.

IV. CONCLUSION

In this paper, we proposed another structure, named DualServer Public Key Encryption with Keyword Search(DSPEKS) that can keep within catchphrase speculatingassault which is an intrinsic vulnerability of the conventionalPEKS structure. We moreover presented another SmoothProjective Hash Function (SPHF) and utilized it to build abland DSPEKS plot. An effective instantiation of the newSPHF in light of the Diffie-Hellman issue is additionallyexhibited in the paper, which gives an effective DS-PEKSplot without pairings.

REFERENCES

[1] R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang, “A new generalframework for secure public key encryption with keyword search,”in Proc. 20th Australasian Conf. Inf. Secur. Privacy (ACISP), 2015,pp. 59–76.

[2] D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searcheson encrypted data,” in Proc. IEEE Symp. Secur. Privacy, May 2000,pp. 44–55.

[3] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, “Order preservingencryption for numeric data,” in Proc. ACM SIGMOD Int. Conf. Manage.Data, 2004, pp. 563–574.

[4] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchablesymmetric encryption: Improved definitions and efficient constructions,”in Proc. 13th ACM Conf. Comput. Commun.Secur.(CCS), 2006,pp. 79–88.

[5] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Publickey encryption with keyword search,” in Proc. Int. Conf. EUROCRYPT,2004, pp. 506–522.

[6] R. Gennaro and Y. Lindell, “A framework for password-basedauthenticated key exchange,” in Proc. Int. Conf. EUROCRYPT, 2003,pp. 524–543.

[7] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, “Building anencrypted and searchable audit log,” in Proc. NDSS, 2004, pp. 1–11.

[8] M. Abdalla et al., "Searchable encryption revisited: Consistencyproperties, relation to anonymous IBE, and extensions," in Proc. 25th Annu. Int. Conf. CRYPTO, 2005, pp. 205–222.

[9] D. Khader, "Public key encryption with keyword search based onK-resilient IBE," in Proc. Int. Conf. Comput. Sci. Appl. (ICCSA), 2006,pp. 298–308.

[10] P. Xu, H. Jin, Q. Wu, and W. Wang, "Public-key encryption withfuzzy keyword search: A provably secure scheme under keywordguessing attack," IEEE Trans. Comput., vol. 62, no. 11, pp. 2266–2277,Nov. 2013.

[11] G. Di Crescenzo and V. Saraswat, "Public key encryption withsearchable keywords based on Jacobi symbols," in Proc. 8th Int. Conf.INDOCRYPT, 2007, pp. 282–296.

[12] C. Cocks, "An identity based encryption scheme based on quadraticresidues," in Cryptography and Coding. Cirencester, U.K.: Springer,2001, pp. 360–363.

[13] J. Baek, R. Safavi-Naini, and W. Susilo, "Public key encryptionwith keyword search revisited," in Proc. Int. Conf. Comput. Sci.Appl. (ICCSA), 2008, pp. 1249–1259.

[14] H. S. Rhee, J. H. Park, W. Susilo, and D. H. Lee, "Improved searchablepublic key encryption with designated tester," in Proc. 4th Int. Symp.ASIACCS, 2009, pp. 376–379.

[15] K. Emura, A. Miyaji, M. S. Rahman, and K. Omote, "Generic constructions of secure-channel free searchable encryption with adaptivesecurity," Secur.Commun.Netw., vol. 8, no. 8, pp. 1547–1560, 2015.