International Journal of Research
Available at https://pen2print.org/index.php/ijr/

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 21
October 2018

An Enhanced Way to Secure Cloud Storage Using Dual-Server Public Key Encryption

Nelaturi Amith Mohan Das, Mrs. M. Veera Kumari
1PG Scholar, Dept.of Computer Science and System Engineering, Andhra University College of Engineering (A), Andhra University, Andhra Pradesh. Student mail id- sanjunelaturi94@gmail.com

2 Research scholar, Dept.of Computer Science and System Engineering , Andhra University College of Engineering (A), Andhra University, Andhra Pradesh. Guide mail id- veerakumarimamidi@gmail.com

Abstract:

Accessible encryption is of extending energy for guaranteeing the data assurance in secure accessible conveyed stockpiling. In this work, we investigate the security of a remarkable cryptographic crude, specifically Public Key Encryption with Keyword Search (PEKS) or, in other words in various usages of dispersed stockpiling. Incredibly, it has been exhibited that the standard PEKS framework encounters a basic unsteadiness called inside Keyword Guessing Attack (KGA) impelled by the malicious server. To address this security helplessness, we propose another PEKS structure named Dual-Server Public Key Encryption with Keyword Search (DS-PEKS). As another principal duty, we describe another variety of the Smooth Projective Hash Functions (SPHFs) implied as straight and homomorphism SPHF (LH-SPHF). We at that point show an insipid advancement of secure DS-PEKS from LH-SPHF. To speak to the likelihood of our new structure, we give a capable instantiation of the general framework from a DDH-based LH-SPHF and show that it can achieve the strong security against inside KGA.

Keywords: Hash Functions, Keyword Guessing Attack, SPHFs, DS-PEKS

1. Introduction

Distributed storage outsourcing has become a widely known application for endeavors and associations to diminish the encumbrance of maintaining cosmically monstrous data as currently. Be that because it could, illogicality, finish shoppers might not by any stretch of the imagination believe the distributed storage servers and will need to encrypt their data before transferring them to the cloud server to defense the data security. This habitually makes the information use more strenuous than the traditional warehousing wherever information is unbroken while not cryptography. One in all the runs of the mill arrangements is that the accessible cryptography that endorses the user to recover the encoded records that contain the utilizer-assigned catchphrases, wherever given the watchword trapdoor, the server will discover the data needed by the user while not unscrambling. Accessible cryptography is often acknowledged in either bilaterally symmetric or uneven cryptography setting. In Melodic synthesis, et al. planned shibboleth looks on figure content, kenned as Accessible bilaterally symmetric cryptography (SSE) and a brief time later some SSE plans were supposed for alterations. Tho' SSE plans savor high effectiveness, they expertise the ill effects of nonplused mystery key dispersion. Shoppers have to be compelled to share mystery keys that are used for data cryptography safely. Else they're not able to enable the disorganized data outsourced to the cloud. To see this downside, Boneh et al. conferred an additional flexible primitive, to be specific Open Key cryptography with Watchword Inquiry (PEKS) that empowers Associate in nursing user to check encoded data within the filter order cryptography setting. In an exceedingly PEKS framework, mistreatment the collector's open key, the sender adds some encoded watchwords (alluded to as PEKS figure writings) with the disorganized data. The collector at that time sends the trapdoor of a to-be-examined shibboleth to the server for data testing. Given the trapdoor and therefore the PEKS figure message, the server will take a look at whether or not the watchword basic the PEKS figure text is indistinguishably similar to the one winnowed by the beneficiary. Providing this is often true, the server sends the coordinative disorganized data to the recipient.

2. Traditional PEKS

Taking after Boneh et al's. Fundamental work, Abdalla et al. formalized unknown IBE (AIBE) and exhibited a nonexclusive development of searchable encryption from AIBE. They likewise demonstrated to exchange a progressive IBE (HIBE) conspire into an open key encryption with brief catchphrase seek (PETKS) where the trapdoor is as it were legitimate in a particular time interim. Waters demonstrated that the PEKS plans in light of bilinear guide could be connected to assemble scrambled and searchable reviewing logs. Keeping in mind the end goal to develop a PEKS secure in the standard model, Khader proposed a plan in view of the k-flexible IBE furthermore gave a development supporting different catchphrase look. The main PEKS plot without pairings was presented by Di Crescenzo and Saraswat . The development is determined from Cock's IBE plot which is not extremely down to earth.

3.RELATED WORK

Cloud computing represents today’s most exciting computing pattern shift in information technology. but, security and privacy are perceived as primary obstacles to its large adoption. Here, outline several critical security challenges and motivate further investigation of security solutions for a trustworthy public cloud environment cloud computing is the latest concept for the long-dreamed vision of computing as a usefulness. It is necessary to store information on information storage servers such as mail servers and record servers in encoded frame to improve security and protection dangers. In any case, this typically suggests one needs to relinquish usefulness for security. For instance, if a customer wishes to recover just reports containing certain words, it was not beforehand known how to let the information stockpilingserver play out the inquiry and answers the question without loss of information secrecy. The issue of seeking on information that is encoded utilizing a public open key framework consider client Bob who sends email to client Alice scrambled under Alice's open key. An email passage needs to test whether the email contains the watchword \urgent" with the goal that it could course the email as needs be. Alice, then again does not wish to give the door the capacity to unscramble every one of her messages. We done and develop an instrument 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 Key Encryption with watchword Search. As another case, consider a mail server that stores different messages openly scrambled for Alice by others. Utilizing our instrument Alice can send the mail server a key that will empower the server to distinguish all messages containing some keyword which is we want to search. 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 Bonehet, al's work, there have been ensuing works that have been proposed to upgrade this idea. Two vital ideas incorporate the 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 extremely constrained, while the last considers the evacuation of secure channel between the beneficiary and the server to make PEKS down to earth. Lamentably, the current development of PEKS secure against catchphrase speculating assault 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 picked catchphrase assault, picked cipher text assault, and against watchword speculating assaults, despite the fact that these thoughts appear to be the most pragmatic use of PEKS primitives. Another 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 cipher text in distinguish ability'.

4.DS-PEKS (Dual Server - Public-key Encryption with Keyword Search):

DS-PEKS theme principally consists of (KeyGen, DS PEKS, DS − Trapdoor, Front-Test, BackTest). To be additional precise, the KeyGen algorithmic rule engenders the public/private key pairs of the front and back servers in part of that of the receiver. Moreover, the trapdoor generation algorithmic rule DS−Trapdoor outlined here is public whereas within the ancient PEKS definition the algorithmic rule Trapdoor takes as input the receiver's non-public key. Such a distinction is as a result of the various structures used by the 2 systems. Within the ancient PEKS, since there's only 1 server if the trapdoor generation algorithmic rule is public, then the server will launch a conjecturing attack against a keyword ciphertext to instaurate the encrypted keyword. As a result, it's impossible to realize the linguistics security. However, as we'll show later, underneath the DS-PEKS framework. Another distinction between the standard PEKS and our planned DSPEKS is that the take a look at algorithmic rule is split into 2 algorithms; Front-Test and Back-Test pass 2 freelance servers. This is often essential for achieving security against the within keyword conjecturing attack. Within the DS-PEKS system, upon receiving a question from the receiver, the front server pre-processes the trapdoor and everyone the PEKS cipher texts utilizing its non-public key, so sends some internal testing-states to the real server with the corresponding trapdoor and PEKS cipher texts obnubilated. The rear server will then decide that documents are queried by the receiver utilizing its non-public key and therefore the received internal testing-states from the front server.

4.1 Algorithm:

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

KeyGen (P): Takes as input the parameters of the system P, outputs the public/secret key pairs (pkFS, skFS), and (pkBS, skBS) for the front server, and therefore the back server respectively;

DS − PEKS (P, pkF S, pkBS, kw1): Takes as input P, the front server's public key pkF S, the rear server's public key pkBS and therefore the keyword kw1, outputs the PEKS ciphertext CTkw1 of kw1;

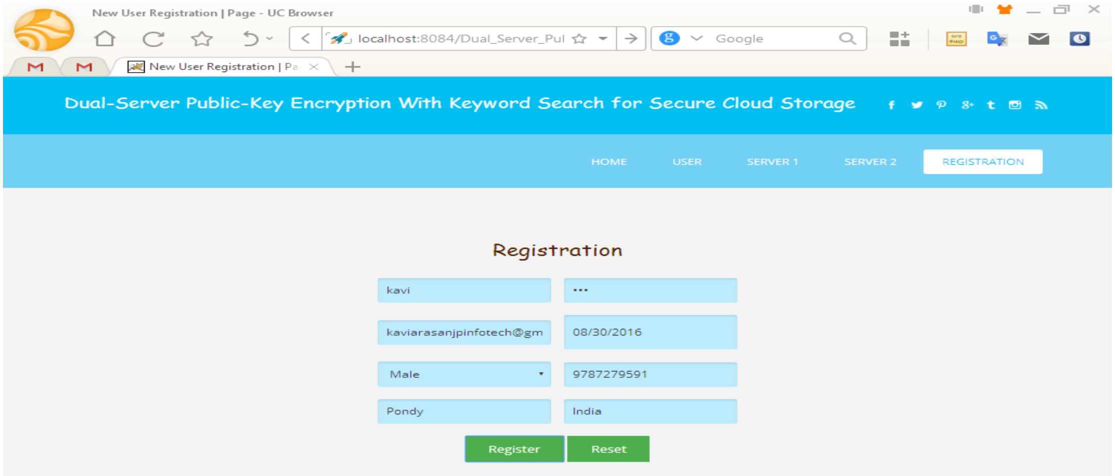
DS − Trapdoor (P, pkF S, pkBS, kw2): Takes as input P, the front server’s public key pkF S, the rear server’s public key pkBS and therefore the keyword kw2, outputs the trapdoor Tkw2;

FrontTest (P, skF S, CTkw1, Tkw2): Takes as input P, the front server’s secret key skF S, the PEKS ciphertext CTkw1 and therefore the trapdoor Tkw2, outputs the interior testing-state CI T S;

BackTest (P, skBS, CI T S): Takes as input P, the rear server’s secret key skBS and therefore the internal testing-state CI T S, outputs testing result zero or 1;

5.Experimental Results

To evaluate the potency of schemes in experiments, we tend to implement the theme utilizing the Java Util packages and recorded the computation time. The subsequent experiments are supported Java.



New User Registration | Page - UC Browser

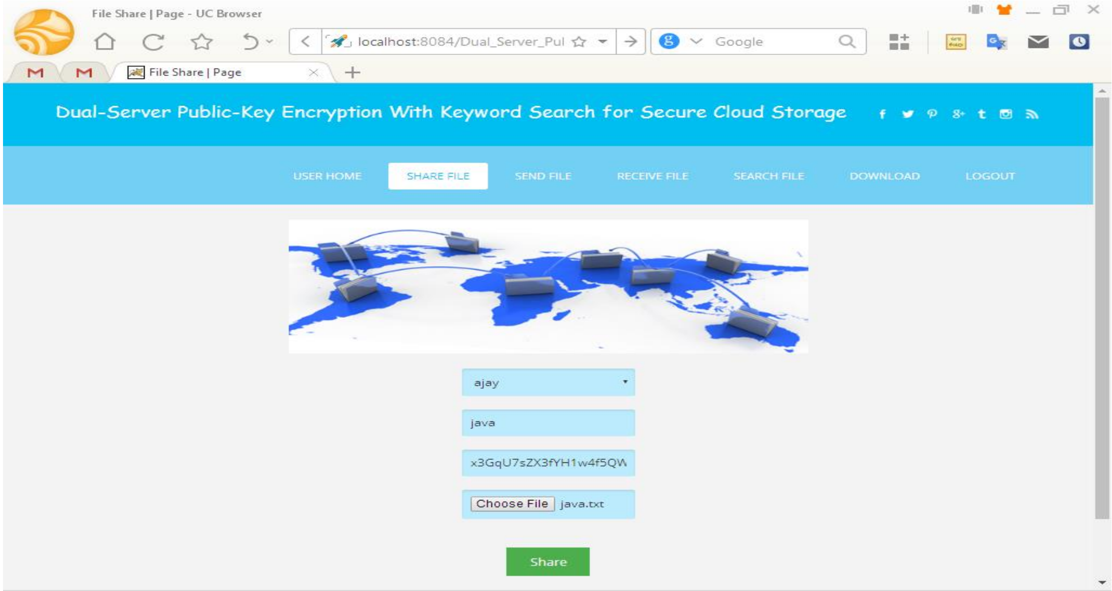
localhost:8084/Dual_Server_Pul

Dual-Server Public-Key Encryption With Keyword Search for Secure Cloud Storage

Registration

kavi
•••
kaviarasanjpinfotech@gm
08/30/2016
Male
9787279591
Pondy
India

5.1 User Registration Form



File Share | Page - UC Browser

localhost:8084/Dual_Server_Pul

Dual-Server Public-Key Encryption With Keyword Search for Secure Cloud Storage

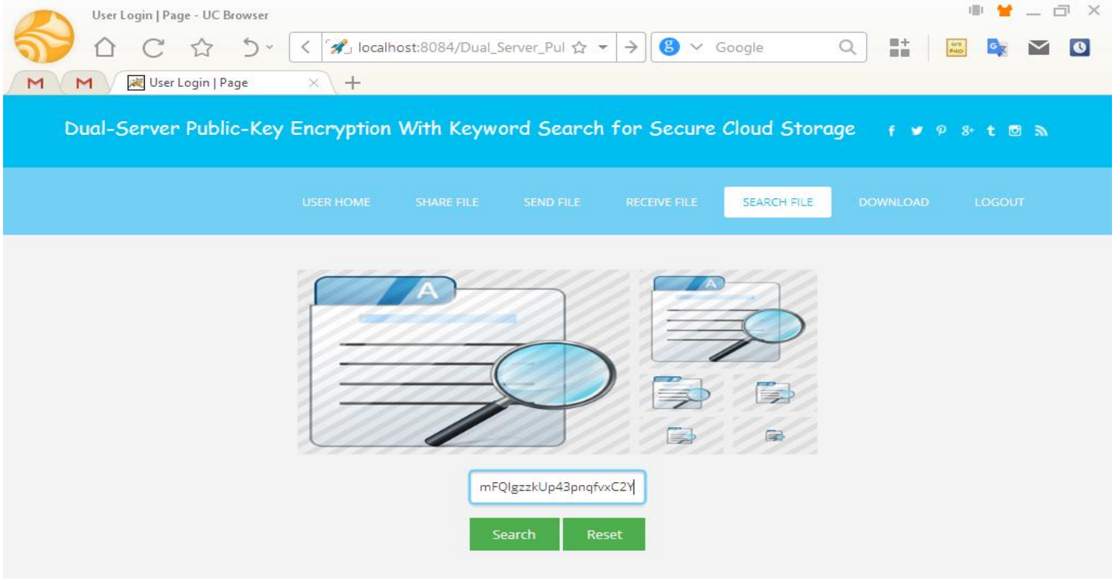
ajay

java

x3GqU7sZX3fYH1w4f5QW

Choose File java.txt

5.2 File Sharing Page



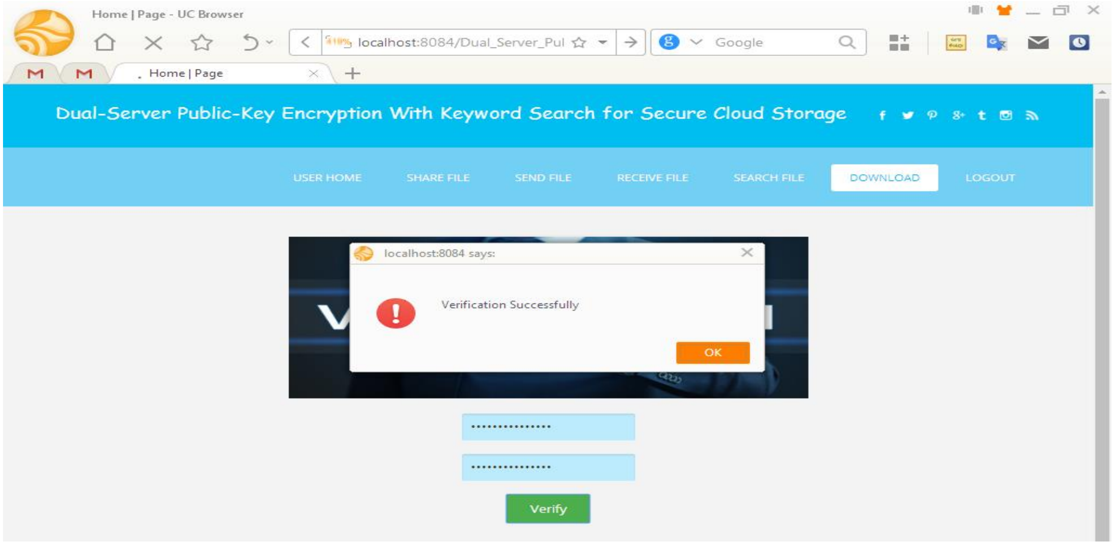
User Login | Page - UC Browser

localhost:8084/Dual_Server_Pul

Dual-Server Public-Key Encryption With Keyword Search for Secure Cloud Storage

mFQIgzzkUp43pnqfvxC2Y

5.3 File Searching Page



Verification Successfully

5.4 File Download Page

6. Conclusions

In this paper, we proposed another structure, named Dual-Server Public Key Encryption with Keyword Search (DSPEKS) that can keep within catchphrase speculating assault which is an intrinsic helplessness of the conventional PEKS structure. We additionally presented another Smooth Projective Hash Function (SPHF) and utilized it to build a bland DSPEKS plot. An effective instantiation of the new SPHF in light of the Diffie-Hellman issue is additionally exhibited in the paper, which gives an effective DS-PEKS plot without pairings.

References

[1] R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang, “A new general framework for secure public key encryption with keyword search,” in Information Security and Privacy - 20th Australasian Conference, ACISP, 2015, pp. 59–76.

[2] D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in IEEE Symposium on Security and Privacy, 2000, pp. 44–55.

[3] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, “Order-preserving encryption for numeric data,” in Proceedings of the ACM SIGMOD International Conference on Management of Data, 2004, pp. 563–574.

[4] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: improved definitions and efficient constructions,” in Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, 2006, pp. 79–88.

[5] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in EUROCRYPT, 2004, pp. 506–522.

[6] R. Gennaro and Y. Lindell, "A framework for password-based authenticated key exchange," in EUROCRYPT, 2003, pp. 524–543.

[7] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, "Building an encrypted and searchable audit log," in NDSS, 2004.

[8] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions," in CRYPTO, 2005, pp. 205–222.

[9] D. Khader, "Public key encryption with keyword search based on k-resilient IBE," in Computational Science and Its Applications - ICCSA, 2006, pp. 298–308.

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

[11] G. D. Crescenzo and V. Saraswat, "Public key encryption with searchable keywords based on jacobi symbols," in INDOCRYPT, 2007, pp. 282–296.

[12] C. Cocks, "An identity based encryption scheme based on quadratic residues," in Cryptography and Coding, 2001, pp. 360–363.

[13] J. Baek, R. Safavi-Naini, and W. Susilo, "Public key encryption with keyword search revisited," in Computational Science and Its Applications - ICCSA, 2008, pp. 1249–1259.

[14] H. S. Rhee, J. H. Park,W. Susilo, and D. H. Lee, "Improved searchable public key encryption with designated tester," in 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 adaptive security," Security and Communication Networks, vol. 8, no. 8, pp. 1547– 1560, 2015.