IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

Double Storage in Cloud Using DS-PEKS

Mubashareen

M.Tech Student, Computer Science Engineering, Maharaja Vijayram Gajapathi Raju College of Engineering, Vizianagaram, India

Abstract: Accessible encryption is of increasing enthusiasm forfending the information protection in secure accessible distributed storage. In this paper, we examine the security of an all around kenned cryptographic primitive, in particular, open key encryption with catchphrase seek (PEKS) which is extremely auxiliary in numerous uses of distributed storage. Haplessly, it has been demonstrated that the customary PEKS system experiences an intrinsically instability called inside watchword guessing assault (KGA) propelled by the threatening server. To address this security weakness, we propose a nascent PEKS system named double server PEKS (DS-PEKS). As another principle commitment, we characterize a beginning variation of the smooth projective hash capacities (SPHFs) alluded to as direct and Homomorphic SPHF (LH-SPHF). We at that point demonstrate a bland development of secure DS-PEKS from LH-SPHF. To outline the possibility of our early system, we give an effective instantiation of the general structure from a Choice Diffie–Hellman-predicated LH-SPHF and demonstrate that it can accomplish the energetic security against inside the KGA.

Keywords: Keyword Search, Secure Cloud Storage, Encryption, Inside Keyword Guessing Attack, Smooth Projective Hash Function, Diffie-Hellman language.

I. INTRODUCTION

Distributed storage outsourcing has turned into a well known application for endeavors and associations to diminish the encumbrance of keeping up cosmically monstrous information as of late. Be that as it may, in validness, end clients may not by any stretch of the imagination believe the distributed storage servers and may want to encode their information before transferring them to the cloud server to defense the information security. This routinely makes the information use more strenuous than the conventional stockpiling where information is kept without encryption. One of the run of the mill arrangements is the accessible encryption which endorses the utilizer to recover the encoded records that contain the utilizer-assigned catchphrases, where given the watchword trapdoor, the server can discover the information required by the utilizer without unscrambling. Accessible encryption can be acknowledged in either symmetric or uneven encryption setting. In Melodic synthesis et al. proposed catchphrase look on figure content, kenned as Accessible Symmetric Encryption (SSE) and a short time later a few SSE plans were intended for alterations. Though SSE plans savor high effectiveness, they experience the ill effects of puzzled mystery key dispersion. Definitely, clients need to safely share mystery keys which are used for information encryption. Else they are not ready to allot the scrambled information outsourced to the cloud. To determine this problem, Boneh et al. presented a more adaptable primitive, to be specific Open Key Encryption with Watchword Inquiry (PEKS) that empowers an utilizer to test encoded information in the hilter kilter encryption setting. In a PEKS framework, using the collector's open key, the sender adds some encoded watchwords (alluded to as PEKS figure writings) with the scrambled information. The collector at that point sends the trapdoor of a to-be-examined catchphrase to the server for information testing. Given the trapdoor and the PEKS figure message, the server can test whether the watchword fundamental the PEKS figure txt is indistinguishably equivalent to the one winnowed by the beneficiary. Provided that this is true, the server sends the coordinating scrambled information to the beneficiary.

II.RELATED WORK

2.1Existing System

Notwithstanding of being free from mystery key dispersion, PEKS plans experience the ill effects of an intrinsically weakness with respect to the trapdoor catchphrase protection, to be specific inside Watchword Guessing Assault (KGA). The reason prompting such security powerlessness is that any individual who kens beneficiary's open key can induce the PEKS ciphertext of self assertive watchword himself. Completely, given a trapdoor, the antagonistic server can winnow a guessing watchword from the catchphrase space and after that use the watchword to cause a PEKS ciphertext. The server at that point can test whether the guessing watchword is the one basic the trapdoor. This guessing then-testing methodology can be emphasized until the point that the right watchword is found. Such a guessing assault has withal been considered in numerous watchword predicated frameworks. In any case, the assailment can be propelled all the more effectively against PEKS plans since the watchword space is generally equipollent to an ordinary

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

lexicon (e.g., all the vital English words), which has a significantly more minute size than a secret key word reference (e.g., every one of the words containing 6 alphanumeric characters). It is significant that in SSE plans, just mystery key holders can induce the catchphrase cipher text and henceforth the antagonistic server is not ready to dispatch within KGA. As the catchphrase dependably betokens the protection of the utilizer information, it is thus of functional significance to surmount this security risk for secure accessible scrambled information outsourcing.

2.2Proposed System

Accessible encryption can be acknowledged in either symmetric or lopsided encryption setting. In Melodic piece et al. proposed watchword look on cipher text, kenned as Accessible Symmetric Encryption (SSE) and a short time later a few SSE plans were intended for improvements. Though SSE plans savor high productivity, they experience the ill effects of astounded mystery key circulation. Absolutely, clients need to safely share mystery keys which are used for information encryption. Else they are not ready to allot the encoded information outsourced to the cloud. To determine this difficulty, Boneh et al. presented a more adaptable primitive, to be specific Open Key Encryption with Catchphrase Inquiry (PEKS) that empowers a utilizer to test encoded information in the uneven encryption setting. In a PEKS framework, using the recipient's open key, the sender joins some scrambled catchphrases (alluded to as PEKS cipher texts) with the encoded information. The collector at that point sends the trapdoor of a to-be-tested catchphrase to the server for information examining. Given the trapdoor and the PEKS cipher text, the server can test whether the catchphrase basic the PEKS cipher text is indistinguishably equivalent to the one winnowed by the recipient. Assuming this is the case, the server sends the coordinating encoded information to the collector.

III. IMPLEMENTATION

3.1Smooth Projective Hash Functions (SPHFs):

Fundamentally, SPHFs are groups of sets of capacities (Hash, ProjHash) characterized on a dialect L. These capacities are filed by a dyad of related keys (hk, hp), where hk, the hashing key, can be optically recognized as the private key and hp, the projection key, as the general population key. On a word W ∈ L, both capacities should prompt indistinguishably equivalent outcome: Hash (hk, L, W) with the hashing key and ProjHash (hp, L, W, w) with the projection key just yet withal a witness w that W ∈ L. Obviously, if W 6∈ L, such a witness does not subsist, and the smoothness property expresses that Hash(hk, L, W) is free of hp. As an outcome, notwithstanding kenning hp, one can't guess Hash (hk, L, W).

3.2Data Owner

It has sizably voluminous data needed to be stored and shared in cloud system. In our scheme, the entity is in charge of defining File keywords and executing file Encrypt operation. And it uploads cipher text to cloud as well keywords (kw) are send to Servers. These two servers can encrypt the keywords and store in cloud.

3.3Data User:

It wants to access an immensely colossal number of data in cloud system. The entity first downloads the corresponding cipher text. Then it executes Decrypt operation of the proposed scheme. Here first afore downloading the cipher text, Data utilizer search with key words then that keywords should be sent to front server, front server can be encrypted that keywords as well as back server additionally can encrypted same key words and probe those keywords in cloud if any keywords are match then encrypted files can be sent to Data utilizer. Data utilizer can be decrypted those files and downloaded.

3.4DS-PEKS (Dual Server - Public key Encryption with Keyword Search):

DS-PEKS scheme mainly consists of (KeyGen, DS − PEKS, DS − Trapdoor, FrontTest, BackTest). To be more precise, the KeyGen algorithm engenders the public/private key pairs of the front and back servers in lieu of that of the receiver. Moreover, the trapdoor generation algorithm DS−Trapdoor defined here is public while in the traditional PEKS definition the algorithm Trapdoor takes as input the receiver's private key. Such a difference is due to the different structures utilized by the two systems. In the traditional PEKS, since there is only one server, if the trapdoor generation algorithm is public, then the server can launch a conjecturing attack against a keyword cipher text to instaurate the encrypted keyword. As a result, it is infeasible to achieve the semantic security. However, as we will show later, under the DS-PEKS framework. Another distinction between the traditional PEKS and our proposed DS-PEKS is that the test algorithm is divided into two algorithms, FrontTest and BackTest run by two independent servers. This is essential for achieving security against the inside keyword conjecturing attack. In the DS-PEKS system, upon receiving a query from the receiver, the front server pre-processes the trapdoor and all the PEKS cipher texts utilizing its private key, and then sends some internal testing-states to the back server with the corresponding trapdoor and PEKS cipher texts obnubilated. The back server can then decide which documents are queried by the receiver utilizing its private key and the received internal testing-states from the front server.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

3.5 Algorithm :

Setup(1λ):

Takes as input the security parameter λ,generates the system parameters P;

•KeyGen(P):

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

• DS − PEKS (P, pkF S, pkBS, kw1):

Takes as input P, the front server's public key pkF S, the back server's public key pkBS and 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 back server's public key pkBS and 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 the trapdoor Tkw2, outputs the internal testing-state CI T S;

• BackTest(P, skBS, CI T S):

Takes as input P, the back server's secret key skBS and the internal testing-state CI T S, outputs testing result 0 or 1;

IV.EXPERIMENTAL RESULTS

To evaluate the efficiency of schemes in experiments, we implement the scheme utilizing the Java Util packages and recorded the computation time. The following experiments are based on Java.

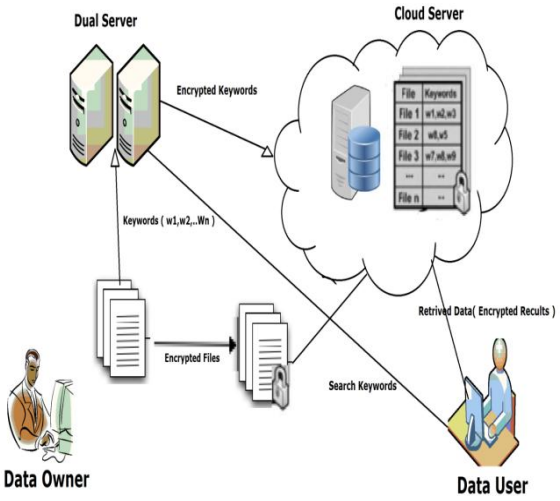

Fig 1 Architecture Diagram

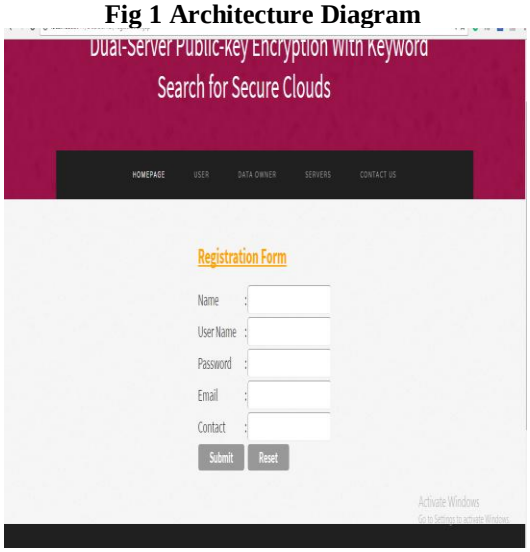

Fig 2 Registration Page

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

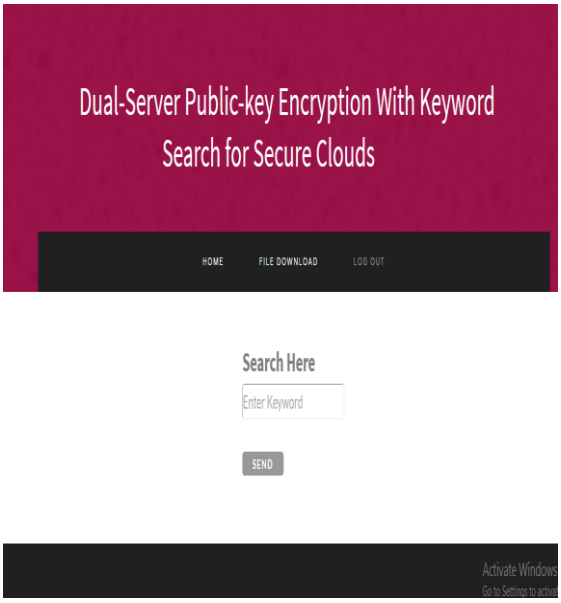

Fig 3 User Search

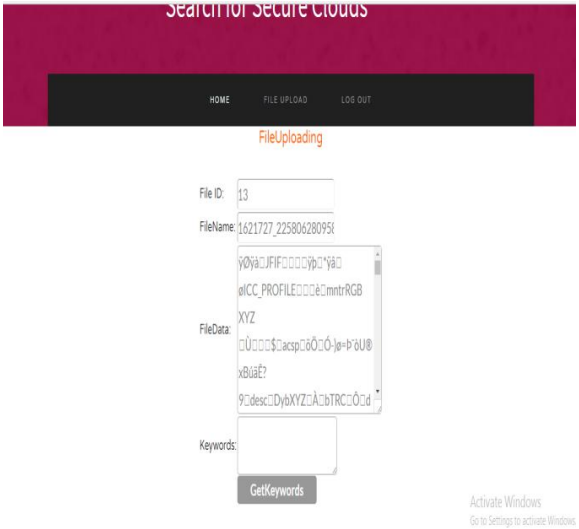

Fig 4 File upload Page

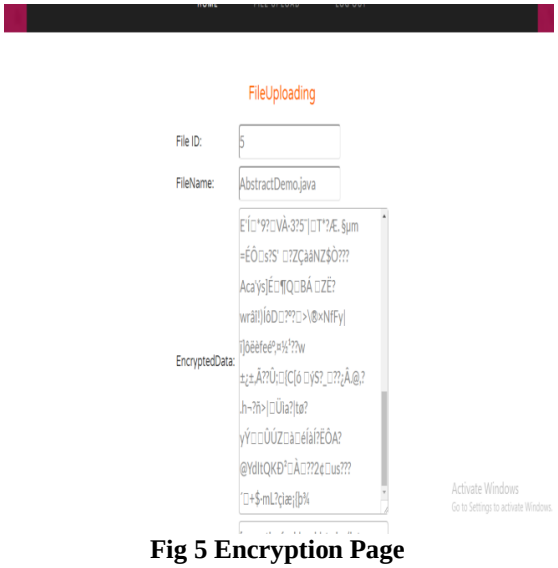

Fig 5 Encryption Page

DOI10.17148/IJARCCE.2017.6637

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

Fig 6DS-PEKS Page

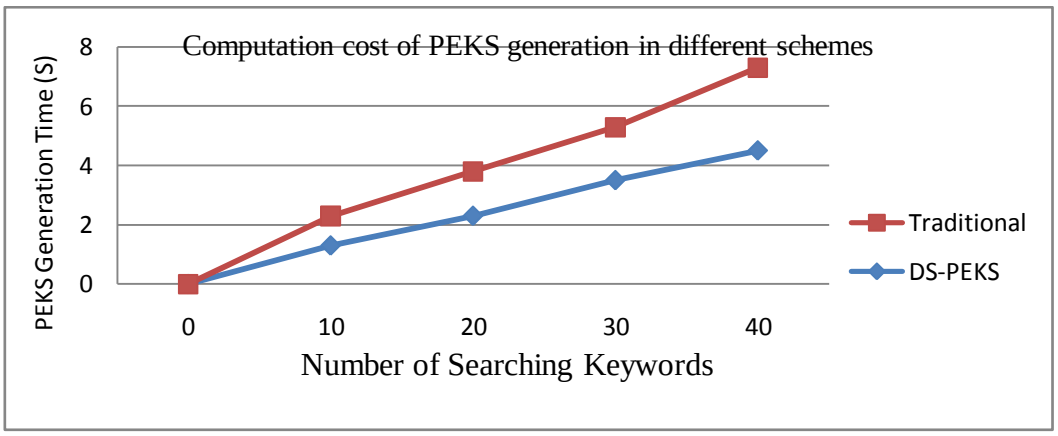

Fig 7 Computation cost of PEKS generation in different schemes

V. CONCLUSION

In this paper, we proposed a beginning structure, designated Double Server Open Key Encryption with Catchphrase Hunt (DS-PEKS), that can deter within watchword guessing assault which is an inborn powerlessness of the conventional PEKS system. We withal presented a nascent Smooth Projective Hash Capacity (SPHF) and used it to develop a non specific DS-PEKS plot. A productive instantiation of the early SPHF predicated on the Diffie-Hellman problem is furthermore displayed in the paper, which gives an effective DS-PEKS conspire without pairings. To better ensure information security, this paper makes the primary endeavor to formally address the issue of tedious for performing Dual Server operations.

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 Proc. 20th Australasian Conf. Inf. Secur. Privacy (ACISP), 2015, pp. 59–76.
[2] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Secur. Privacy, May 2000, pp. 44–55.
[3] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption 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, "Searchable symmetric 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, "Public key encryption with keyword search," in Proc. Int. Conf. EUROCRYPT, 2004, pp. 506–522.
[6] R. Gennaro and Y. Lindell, "A framework for password-based authenticated key exchange," in Proc. Int. Conf. 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 Proc. NDSS, 2004, pp. 1–11.
[8] M. Abdalla et al., "Searchable encryption revisited: Consistency properties, 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 on K-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 with fuzzy keyword search: A provably secure scheme under keyword guessing attack," IEEE Trans. Comput., vol. 62, no. 11, pp. 2266–2277, Nov. 2013.