Impact Factor Value: 4.029 ISSN: 2349-7084
International Journal of Computer Engineering In Research Trends
Volume 4, Issue 10, October-2017, pp. 419-423 www.ijcert.org

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

[1] **Anjum Saba Afsheen**, [2] **Dr. G.S.S Rao**
[1]Pursuing M.Tech(CSE), [2]Professor & HOD
[1,2]Nawab ShahAlam khan College of Engineering and Technology, Hyd
Email: anjumsaba57@gmail.com,profgssrao@gmail.com

Abstract: Accessible cryptography is of accelerating enthusiasm for fending the data protection in secure, accessible distributed storage. During this paper, we tend to examine the safety of Associate in Nursing all-round kenned cryptological primitive, above all, open key cryptography with shibboleth ask for (PEKS) that is extraordinarily auxiliary in varied uses of distributed storage. Haplessly, it's been incontestable that the customary PEKS system experiences Associate in Nursing essential instability referred to as within watchword approximation assault (KGA) propelled by the threatening server. To deal with this security weakness, we tend to propose an aborning PEKS system named double server PEKS (DS-PEKS). As another principle commitment, we tend to characterize a starting variation of the graceful projective hash capacities (SPHFs) alluded to as direct and Homomorphic SPHF (LH-SPHF). We tend to at that time demonstrate a bland development of secure DS-PEKS from LH-SPHF. To stipulate the chance of our early system, we tend to offer a good representation of the final structure from a selection Diffie–Hellman-predicated LH-SPHF and demonstrate that it will accomplish the energetic security against within the KGA.

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

---

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.Related Work

2.1 Existing System

Notwithstanding of being free from mystery key dispersion, PEKS plans to expertise the unwell effects of Associate in Nursing essential weakness concerning the trapdoor shibboleth protection, to be fixed within Watchword approximation Assault (KGA). The rationale prompting such security impotence is that somebody UN agency kens beneficiary's open key will induce the PEKS ciphertext of self-assertive watchword himself. Completely, given a trapdoor, the antagonistic server will winnow an approximation watchword from the shibboleth house and subsequently use the watchword to cause a PEKS ciphertext. The server at that time will take a look at whether or not the approximation watchword is that the one basic the trapdoor. This approximation then-testing methodology is often emphasized till the purpose that the proper watchword is found. Such an approximation assault has nonetheless been thought of in varied watchword predicated frameworks. In any case, the offenders often propelled all the additional effectively against PEKS plans since the watchword house is usually equipollent to a standard lexicon (e.g., all the important English words), that incorporates a considerably additional minute size than a secret keyword reference (e.g., each one of the words containing half dozen alphanumerical characters). It's important that in SSE plans, simply mystery key holders will induce the shibboleth ciphertext and henceforward the antagonistic server isn't able to dispatch at intervals KGA. Because the shibboleth reliably betokens the protection of the user data, it does therefore of practical significance to surmount this security risk for secure, accessible disorganized data outsourcing.

2.2 Proposed System

Accessible cryptography is often acknowledged in either bilaterally symmetric or lopsided cryptography setting. In Melodic piece et al. planned watchword look on ciphertext, kenned as Accessible bilaterally symmetric cryptography (SSE) and a brief time later some SSE plans were supposed for enhancements. Tho' SSE plans savor high productivity, they expertise the unwell effects of amazed mystery key circulation. Shoppers have to be compelled to safely share mystery keys that are used for data cryptography. Else they're not able to enable the encoded data outsourced to the cloud. To see this problem, Boneh et al. conferred an additional flexible primitive, to be specific Open Key cryptography with shibboleth Inquiry (PEKS) that empowers a used to check encoded data within the uneven cryptography setting. in an exceedingly PEKS framework, mistreatment the recipient's open key, the sender joins some disorganized catchphrases (alluded to as PEKS ciphertexts) with the encoded data. The collector at that time sends the trapdoor of a to-be-tested shibboleth to the server for data examining. Given the trapdoor and therefore the PEKS ciphertext, the server will take a look at whether or not the shibboleth basic the PEKS ciphertext is indistinguishably similar to the one winnowed by the recipient. Assumptive this is often the case; the server sends the coordinative encoded data to the collector.

3. Implementation

3.1 Smooth Projective Hash Functions (SPHFs):

Fundamentally, SPHFs are teams of sets of capacities (Hash, ProjHash) characterized on an idiom L. These capacities are filed by a yoke of connected keys (hk, hp), where hk, the hashing key, are often optically recognized because the non-public key and horsepower, the projection key, because the general population key. On a word W ∈ L, each capacity ought to prompt indistinguishably equivalent outcome: Hash (hk, L, W) with the hashing key and ProjHash (hp, L, W, w) with the projection key simply nonetheless nonetheless a witness w that W ∈ L. Obviously, if W 6∈ L, such a witness doesn't exist, and therefore the smoothness property expresses that Hash (hk, L, W) is freed from horsepower. As Associate in the nursing outcome, however, the figure of speech horsepower, one cannot guess Hash (hk, L, W).

3.2 Data Owner

It has the sizably voluminous information required to be held on and shared within the cloud system. In our theme, the entity is to blame of shaping File keywords and execution file inscribe operation. And it uploads ciphertext to cloud also keywords (kw) are send to Servers. These 2 servers will inscribe the keywords and store within the cloud.

3.3 Data User: It needs to access a massive variety of knowledge in the cloud system. The entity initial downloads the corresponding ciphertext. Then it

executes decode operation of the planned theme. Here initial afore downloading the ciphertext, information user search with keywords then that keywords ought to be sent to front server, front server is often encrypted that keywords also as back server to boot will same encrypted keywords and probe those keywords in cloud if any keywords are matched then encrypted files are often sent to information user. Information user has often decrypted those files and downloaded.

3.4 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.

3.5 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;

4.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.

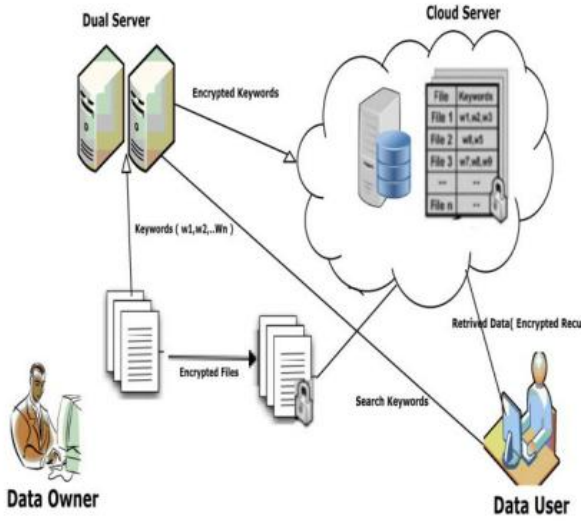

Fig 1 Architecture Diagram

Fig 2 Registration Page

Fig 3 User Search

Fig 4 File upload Page

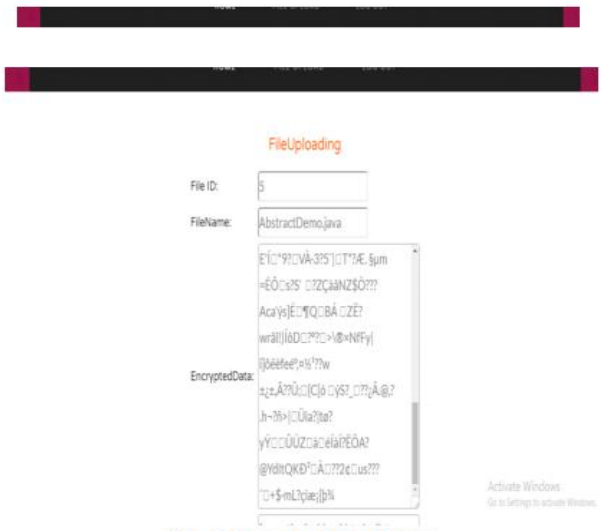

Fig 5 Encryption Page

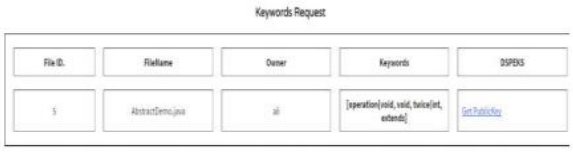

Fig 6DS-PEKS Page

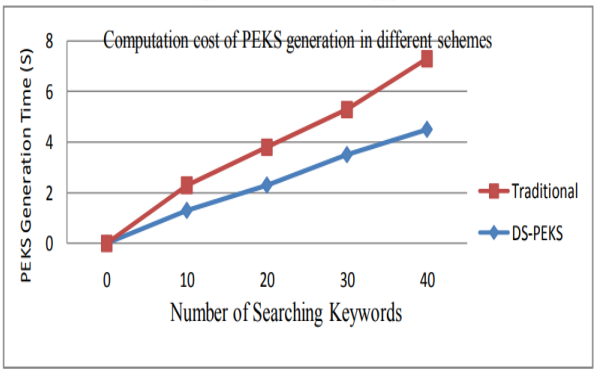

Fig 7 Computation cost of PEKS generation in different schemes

5. Conclusion

In this paper, we tend to plan a starting structure, selected Double Server Open Key cryptography with shibboleth Hunt (DS-PEKS), which will deter at intervals watchword approximation assault that is Associate in nursing inborn impotence of the traditional PEKS system. We tended to nonetheless conference aborning sleek Projective Hash capability (SPHF) and used it to develop a non-specific DS-PEKS plot. A productive representation of the first SPHF predicated on the Diffie-Hellman downside is what is more displayed within the paper, which provides a good DS-PEKS conspire while not pairings. To raised guarantee data security, this paper makes the first endeavor to formally address the difficulty of tedious for playacting twin 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. Secure. Privacy (ACISP), 2015, pp. 59–76.

[2] P. Xu, H. Jin, Q. Wu, and W. Wang, "Public-key encryption with a fuzzy keyword search: A provably

secure scheme under keyword guessing attack," IEEE Trans. Comput., vol. 62, no. 11, pp. 2266–2277, Nov. 2013.

[3] 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.

[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] 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.

[6] 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.

[7] 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.

[8] 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.

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

[10] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Secure. Privacy, May 2000, pp. 44–55.

[11] A.Raghavendra Praveen Kumar, K.Tarakesh, and U.Veeresh ," A Secure and Dynamic Multi Keyword Ranked Search Scheme over encrypted." International Journal of Computer Engineering in Research Trends., vol.2, no.12, pp. 1137-1141, 2015.

[12] Mr. Rahul Hon, and Mrs. N.Sujatha," A Novel Framework to Measure the Degree of Difficulty on Keyword Query Routing." International Journal of Computer Engineering in Research Trends., vol.3, no.6, pp. 314-320, 2016.

[13] Kallem Rajender Reddy, and Y.Sunitha," A Novel Framework to Measure the Degree of Difficulty on Keyword Query Routing." International Journal of Computer Engineering in Research Trends., vol.2, no.9, pp. 640-645, 2015.

[14] Vadla Jhansi Rani, and K.Samson Paul," Secure Multi Keyword Dynamic Search Scheme Supporting Dynamic Update.." International Journal of Computer Engineering in Research Trends., vol.4, no.8, pp. 356-360, 2017.

[15] Mr. M. Veerabrahma Chary and Mrs.N.Sujatha," A Novel Additive Multi-Keyword Search for Multiple Data Owners in Cloud Computing." International Journal of Computer Engineering in Research Trends., vol.3, no.6, pp. 308-313, 2016.

[16] Mr. M. VEERABRAHMA CHARY, Mrs.N.SUJATHA," A Novel Additive Multi-Keyword Search for Multiple Data Owners in Cloud Computing ." International Journal of Computer Engineering In Research Trends., vol.3, no.6, pp. 308-313, 2016.

[17] G.Lucy, D.Jaya Narayana Reddy, R.Sandeep Kumar," Enabling Fine-grained Multi-keyword Search Supporting Classified Sub-dictionaries over Encrypted Cloud Data." International Journal of Computer Engineering In Research Trends., vol.2, no.12, pp. 919-923, 2015.

[18] G.Dileep Kumar, A.Sreenivasa Rao," Privacy-Preserving Public Auditing using TPA for Secure Searchable Cloud Storage data." International Journal of Computer Engineering In Research Trends., vol.2, no.11, pp. 767-770, 2015.

