Applied GIS

ISSN: 1832-5505
Vol-10 Issue-01 Jan 2022

Secure Cloud Storage with Keyword Search and Dual Server Public Key Encryption

D. SNEHA, Assistant Professor, sneha.dharmavaram@gmail.com

K. BALAJI SUNIL CHANDRA, Professor, hod.cse@svitatp.ac.in

VIJAYA BHASKAR MADGULA, Professor, vijaya.bhaskar2010@gmail.com

Department of CSE, Sri Venkateswara Institute of Technology,

N.H 44, Hampapuram, Rapthadu, Anantapuramu, Andhra Pradesh 515722

Abstract:

To guarantee data security in safe, distributed storage, accessible cryptography is becoming more common. A widely used cryptographic fundamental in many distributed storage systems, public key cryptography with shibboleth request (PEKS) is the focus of this study's investigation of its security. It has been shown that the typical PEKS system has a serious flaw called inner watchword approximation attack (KGA), which is set off by the malicious server. Double server PEKS (DS-PEKS) is an emerging PEKS solution that we propose to fix this security hole. Instead of using the abbreviation "LH-SPHF," we'd rather use "SPHF" to refer to a basic form of graceful projective hash capacities (SPHFs) that is direct and homomorphic. At that point, we often demonstrate a boring progression of secure DS-PEKS from LH-SPHF. just now. We provide a reasonable description of the final structure based on a Diffie-Hellman-based LH-SPHF and demonstrate that it will attain energy security within the KGA to demonstrate the feasibility of our first system

.

Introduction

1. The term "cloud computing" refers to the practice of accessing computer programmes and hardware over a shared network, most often the Internet. The term is derived from the fact that cloud-shaped symbols are often used in system diagrams to represent the complex architecture they comprise. Users' data, software, and processing are entrusted to distant services in cloud computing. In cloud computing, resources (including software and hardware) are made accessible via the Internet as services (controlled by a third party). In most cases, these services provide users access to sophisticated computer programmes and networks of server machines. With cloud computing, a popular example in the field of computer science and related fields. Access to a common pool of reconfigurable system resources is made simple. It requires little to no effort to handle. It offers both accessibility and security at the same time. Computing in the cloud refers to the practice of delivering services via a shared pool of remote computer resources. It gives third-party services access to user information, programmes, and computations. There was a risk of theft for the data kept by a third-party system. Data protection necessitates encryption, which was still a problem with conventional PEKS. It inspired the development of DS-PEKS, a more secure method of storing data in the cloud.

ISSN: 1832-5505
Vol-10 Issue-01 Jan 2022

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

ISSN: 1832-5505
Vol-10 Issue-01 Jan 2022

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.

Implementation

2.3 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 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).

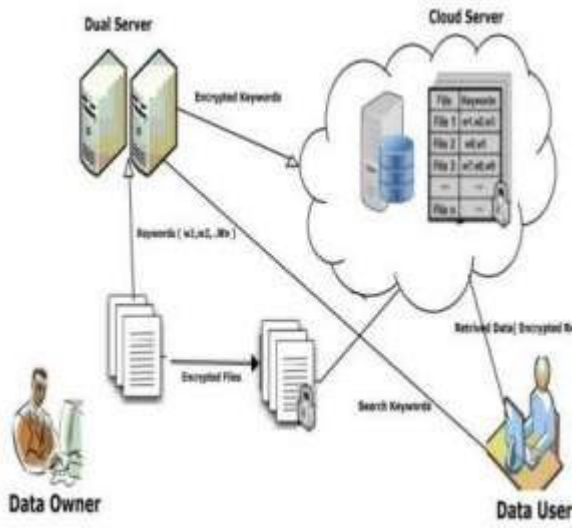


Fig-1. System Architectural Design

ISSN: 1832-5505
Vol-10 Issue-01 Jan 2022

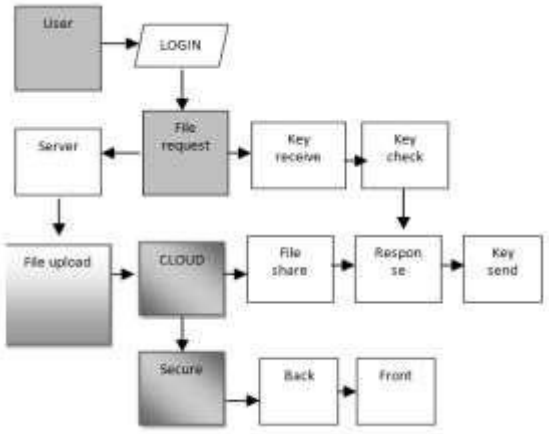


Fig-2. Data Flow Diagram

2.4 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.

2.5 Data User:

It needs to access a massive variety of knowledge in the cloud system. The entity initial downloads the user has often decrypted those files and downloaded.

2.6 DS-PEKS (Dual Server - Public-

DS-PEKS theme principally consists of (Key Gen, DS− PEKS, DS − Trapdoor, Front-Test, Back Test). To be additional precise, the Key Gen algorithmic rule

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

key Encryption with Keyword Search):

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

ISSN: 1832-5505
Vol-10 Issue-01 Jan 2022

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

Key Gen (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; Front Test (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;

Back Test (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;

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.

2.7 Algorithm:

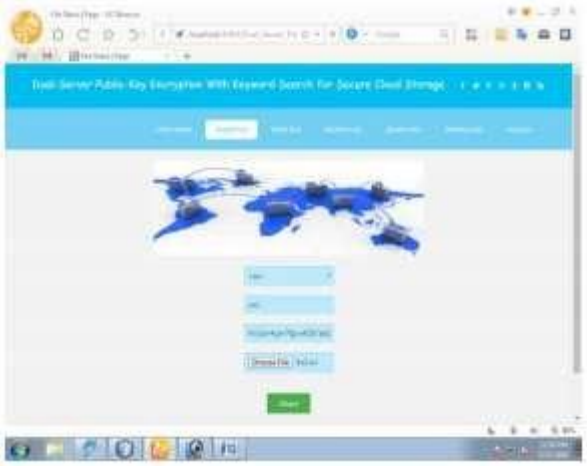
3. Experimental Results

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

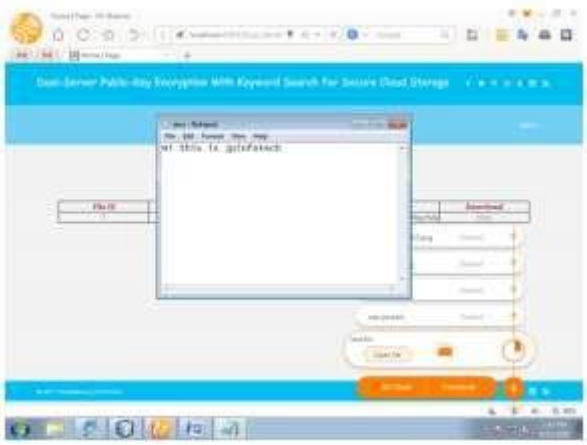
ISSN: 1832-5505
Vol-10 Issue-01 Jan 2022

Java.

a) User Registration:



b) User Login:



ISSN: 1832-5505
Vol-10 Issue-01 Jan 2022

4. Conclusion

In order to circumvent the inherent weakness of the conventional PEKS system—word approximation attacks—in this study, we propose a foundational framework called DS-PEKS, which stands for Double Server Open Key cryptography with shibboleth Hunt. We still met and used aborning smooth Projective Hash function (SPHF) to create a generic DSPEKS graphic. The study also displays an effective depiction of the first SPHF based on the Diffie-Hellman disadvantage, which gives a decent DS-PEKS conspire without pairs. This work explicitly addresses the challenge of playing out dual Server operations in an effort to increase data security guarantees.

References

"Searchable symmetric encryption: Improved definitions and efficient constructions," which can be found on pages 79–88.\ The paper "Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions" was published in 2005 in the proceedings of the 25th Annual International Conference on Cryptography (CRYPTO). In the 2004 Proc. NDSS, B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters discussed the development of an encrypted and searchable audit log (pp. 1-11). [7] "Public key encryption with keyword search," in Proceedings of the 2004 International Conference on Cryptography, pages 506-522, by D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano. The paper "Order preserving encryption for numeric data" was presented at the 2004 ACM SIGMOD International Conference on Management Data and authored by R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu. "A

[1] Proc. 20th Australasian Conf. Inf. Secure. Privacy (ACISP), 2015, pp. 59–76, "A new general framework for secure public key encryption with keyword search" (R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang). A provably secure technique under keyword guessing attack: public-key encryption with a fuzzy keyword search, by P. Xu, H. Jin, Q. Wu, and W. Wang The IEEE Computer Science, volume 62, issue 11, pages 2266–2277, November 2013. “Public key encryption with keyword search based on K-resilient IBE” (D. Khader, 2006, pp. 298-308) was presented at the 2006 International Conference on Computer Science and Applications (ICCSA). [4] In the proceedings of the thirteenth Annual ACM Conference on Computer Security (CCS), 2006, R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky presented

ISSN: 1832-5505
Vol-10 Issue-01 Jan 2022

framework for password-based authenticated key exchange," in Proc. Int. Conf. EUROCRYPT, 2003, pp. 524-543, was written by R. Gennaro and Y. Lindell. In the proceedings of the IEEE Symposium on Security and Privacy, May 2000, D. X. Song, A. Perrig, and D. Wagner presented "Practical techniques for searches on encrypted data," which may be found on pages 44–55.