Secure File Storage in Cloud Computing Using Dual Server Encryption and Decryption Techniques

K. Siri Chandana, B.Nirmala, G.Sai Neelima

ABSTRACT— Searchable encryption is of increasing enthusiasm for guaranteeing the advantage safeguard in comfortable available distributed storage. In the course of this work, we are likely to compare the safeguard of an outstanding cryptologic crude, to be unique Public Key Encryption with Keyword Search (PEKS) that's terribly useful in more than a few makes use of-of allotted storage. Sadly, it's been incontestable that the normal PEKS structure experiences a characteristic uncertainty referred to as inside keyword Guessing attack (KGA) propelled through the malignant server. To control this security weak spot, we are likely to suggest one more PEKS constitution named twin-Server Public Key Encryption with key phrase Search (DS-PEKS). As yet another long-established obligation, To delineate the likelihood of our new process, we are likely to supplies an informed intellectual illustration of the total structure from a DDH-founded LH-SPHF and show that it's going to accomplish the stable protection towards inside KGA.

Index Terms— key phrase search, relaxed cloud storage, encryption, inside of keyword guessing assault, gentle projective hash perform, Diffie-Hellman language.

I. INTRODUCTION

Cloud storage outsourcing has become a favored software for businesses and businesses to lessen the burden of maintaining gigantic capabilities in contemporary years. Nonetheless, surely, finish users might now not completely trust the cloud storage servers and will select to write down their potential earlier than uploading them to the cloud server in an effort to shield the information privacy. The files stored in the Data Base are encrypted using Data Encryption Standard (DES) algorithm. Using randomization process the public key is sent to receiver. Using this public key the receiver searches the file and request the double servers to access the required file. Then the both servers sends the different randomized private keys to receiver's mail. The Simple Mail Transfer Protocol (SMTP) is used to send the mails which contains two secret keys and authenticated using Secure Socket Layer (SSL) which provides firewall protection to send keys. Using these private keys which are received to receiver's mail, the receiver can download the file if these two different private keys are matched. The file is then decrypted and downloaded successfully.

II. RELATED WORK

2.1 Proposed System

In this, we proposed a new procedure known as relaxed File Storage in Cloud Computing making use of twin Server Encryption and Decryption strategies to address the security of PEKS. A brand new variant of glossy Projective Hash function referred to as linear and homomorphic SPHF, is offered for an ordinary construction of DS-PEKS .To demonstrate the usefulness of our new framework, accomplice competitively priced illustration of our SPHF supported the Diffie-Hellman is used. DES algorithm is used for each encryption and decryption method. Double servers are used to generate extremely secured exclusive keys. SMTP-SSL protocols are used for producing mail and firewall safety. The algorithms used in these tasks are DES. As one other foremost contribution, we define a brand new variant of smooth Projective Random operate (SPRF) which generates extraordinary keys for sharing records. Documents are decrypted utilizing general algorithm DES. This undertaking also indicates an established development of relaxed Mail generation making use of SMTP which share keys and supplies strong safety in opposition to KGA.

Searchable coding is of growing curiosity for safeguarding the information privacy in relaxed searchable cloud storage. For the period of this paper, we tend to investigate the protection of a greatly known scientific self-discipline primitive, specifically, public key coding with key phrase search (PEKS) that's incredibly important in a couple of purposes of cloud storage. Alas, it can be been proven that the traditional PEKS framework suffers from associate inherent insecurity referred to as inside key phrase guesswork assault (KGA) launched via the malicious server. To take care of this safety vulnerability, we are inclined to advocate a manufacturer new PEKS framework named twin-server PEKS (DS-PEKS). As yet another major contribution,

III. LITERATURE SURVEY

We are likely to define a manufacturer new variant of the smooth projective hash services (SPHFs) mentioned as linear and homomorphic SPHF (LH-SPHF). Let's assume

Revised Manuscript Received on April 05, 2019.

K. Siri Chandana UG Scholar, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Thandalam, Chennai, Tamilnadu, India- 602 105.

B. Nirmala Assistant Professor, Faculty of Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Thandalam, Chennai, Tamilnadu, India-602105.

G. Sai Neelima UG Scholar, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Thandalam, Chennai, Tamilnadu, India- 602 105.

the practicability of our new framework, we offer companion efficient inner illustration of the final framework from an alternative Diffie–Hellman-established LH-SPHF and exhibit that it is competent to do the sturdy safety against inside the KGA [1].

Accessible cryptography is of quick enthusiasm for fending the competencies security in comfy, available dispensed storage. Throughout this paper, we generally tend to are likely to tend to appear on the safeguard of a companion in Nursing comprehensive kenned science primitive, primarily, open key cryptography with shibboleth kindle (PEKS) that's relatively auxiliary in diverse makes use of-of dispersed storage. To upset this protection weakness, we tend to are inclined to tend to endorse accomplice parturient PEKS procedure named double server PEKS (DS-PEKS). We tend to are inclined to be likely to at the moment show bland progress of relaxed DS-PEKS from LH-SPHF. To stipulate the possibility of our early system, we generally tend to are likely to tend to furnish companion honest illustration of the ultimate word structure from a spread Diffie-Hellman-predicated LH-SPHF and demonstrate that it'll accomplish the vigorous safety towards within the KGA [2].

Knowledge sharing may be a critical utility in a cloud environment. This information can be extra useful to cooperating corporations in the event that they had been in a position to share their information. For the duration of this article, accomplice reasonable methodology is supplied to firmly, with effectivity, and flexibly share data with others in cloud computing, however, the replacement encrypted records outside the set preserve private. Comfy study kind and dealing methodology unit of dimension projected in the course of this paper for quality services over the cloud [3].

In this paper it allows for a third occasion realizing the hunt trapdoor of a keyword to appear encrypted files containing that keyword whereas no longer decrypting the files or understanding the key phrase. Nonetheless, it is proven that the key phrase is traveling be compromised by using a malicious third occasion below a key phrase bet assault (KGA) if the key phrase area is for the duration of a polynomial measurement. We address this drawback with a keyword privacy amassed variant of PEKS aforementioned as public-key secret writing with fuzzy keyword search (PEFKS).A pair of or extra key terms share the same fuzzy keyword trapdoor. To travel looking encrypted records containing a particular key phrase, simplest the fuzzy key phrase search trapdoor is supplied to the 0.33 celebration, i.e., the searcher. Accordingly, in PEFKS, a malicious searcher can no longer be trained the unique key phrase to be searched withal the keyword house could be very little. We have now a bent to recommend a common transformation that converts any anonymous identification-headquartered secret writing (IBE) theme into a secure PEFKS theme. Following the typical development, we now have an unethical to instantiate the first PEFKS theme tried to be relaxed at a lower location KGA among the case that the keyword residence is in accomplice particularly polynomial dimension [4].

Notions of security and schemes for symmetrical (i.e. ~confidential key) secret writing in associate totally concrete security framework. Now we have a bent to deliver several utterly entirely unique notions of security and analyze the concrete high-quality of markdowns among them. [5]

New tactics for remote reckoning on encrypted understanding sample companion in nursing untrusted server and furnished proofs of safety for the next crypto methods. Our techniques have sort of relevant advantages: they may be demonstrably cozy; they help controlled and hidden search and query isolation; they are effortless and speedy (more specifically, for a file of length n, the key writing and search algorithms handiest would love O (n) flow cipher and block cipher operations); which they introduce just about no house and communique overhead. Our theme is as well particularly flexible, and it is going to merely be elevated to help additional developed search queries. We tend to are likely to conclude that this provides a sturdy new constructing block for the occasion of comfy services among the many untrusted infrastructures [6].

In this the person Bob World health organization sends email to user Alice encrypted underneath Alice's public key. Alice, on the alternative hand, does not would really like to relinquish the entree the flexibleness to decipher all her messages. We tend to tend to stipulate and construct a mechanism that permits Alice to furnish a key to the entree that makes it possible for the entranceway to test whether or now or not the phrase "pressing" may just well be a key phrase at intervals the email whereas now not finding out anything on the subject of the email. We are likely to be inclined to determine this mechanism as Public Key secret writing with key phrase Search. As one more instance, think about a mail server that retailers various messages publically encrypted for Alice by way of others [7].

Searchable symmetric secret writing (SSE) allows a get together to give the storage of his knowledge to a special occasion in a passing manner, whereas keeping the flexibleness to selectively search over it. This disadvantage has been the most focal point of energetic evaluation and sort substitute protection definitions and constructions are deliberate. For the period of this paper, we tend to begin through reviewing existing notions of protection and endorse new and stronger security definitions. We are inclined to tend to then reward two constructions that we tend to denote comfy underneath our new definitions. It appears, to boot to pleasant superior protection guarantees, our constructions rectangular measure further efficient than all earlier constructions [8].

A basic framework for password-based actual key alternate protocols, at intervals the customary reference string mannequin. Our protocol is honestly partner in nursing abstraction of the key alternate protocol of Katz et al. And is based on the lately offered proposal of sleek projective hashing via Cramer and Shop. We are likely to understand a variety of benefits from this abstraction. First, we are likely to tend to amass a typical protocol so that they can be portrayed pattern basically three excessive-stage subject tools. This allows for a convenient and intuitive working out of its security. 2nd, our proof of security is

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

significantly simpler and extra-natural. Third, we tend to are likely to rectangular measure ready to derive analogs to the Katz et al. Protocol beneath additional field assumptions. Accordingly on realize this, we tend to assemble new sleek projective hash services [9].

Cloud computing is popping into predominant; information house owners rectangular measure driven to delegate advanced advantage managements to the trade cloud for fiscal financial savings. Sensitive know-how is frequently encrypted earlier than being uploaded to the cloud that sadly makes the quite often-used search operate a hard drawback. In the course of this paper, we tend to are likely to gift a replacement multi-key phrase dynamic search theme with outcomes ranking to appear encrypted understanding safer and smart. For the priority of efficiency, we are inclined to be likely to undertake a tree-established index constitution to facilitate the trying system and alter operations. A complete protection evaluation is furnished, and experiments over the $64000 world know-how exhibit that our theme is inexpensive [10].

IV. IMPLEMENTATION

3.1 knowledge Owner: Register with cloud server and login (username should be unique). Send request to Public key generator (PKG) to get Key on the user name. Browse file and request Public key to encode the information, transfer knowledge to cloud service supplier. Verify the information from the cloud.

3.2 Public key generator: Receive request from the users to get the key, store all the keys supported user names. Check the user name and supply the personal key.

3.3 Key Update: Receive all files from the information owner and store all files. Check the information integrity within the cloud and inform to the tip user regarding the data integrity .Send request to PKG to update the personal key of the user supported the date parameter.

3.4 Entrance Server: After receiving the query from the receiver, the entrance server pre-strategies the trapdoor and every person the PEKS cipher texts victimization its private key, and so sends some interior trying out-states to the real server with the corresponding trapdoor and PEKS cipher texts hidden.

3.5 Again Server: for the period of this module, the again server will then come to a decision that files are queried by the receiver victimization its individual key and accordingly the obtained internal checking out-states from the entrance server.

3.7 DS-PEKS (dual Server - Public key cryptography with key phrase Search): DS-PEKS theme usually consists of (Key Gen, DS − PEKS, DS − Trapdoor, front list, Back Test). To be extra distinct, the key Gen formulation engenders the general public/personal key pairs of the front and back servers in the workplace of that of the receiver. Additionally, the trapdoor new release formulation DS−Trapdoor printed right here is public whereas throughout the common PEKS definition the components Trapdoor takes as input the receiver's private key.

Any such difference is due to the various constructions utilized through the 2 systems. Throughout the average PEKS, for the reason that there's only one server, if the trapdoor new release formula is public, then the server can launch a conjecturing assault in opposition to a keyword cipher textual content to instauration the encrypted key phrase. For that reason, it is not feasible to recognize linguistics safety. Nevertheless, as we will exhibit later, under the DS-PEKS framework. This can be most important for achieving safety in opposition to the within key phrase conjecturing assault. Inside the DS-PEKS approach, upon receiving a topic from the receiver, the front server pre-procedures the trapdoor and everyone the PEKS cipher texts utilizing its personal key, therefore sends some inside testing-states to the real server with the corresponding trapdoor and PEKS cipher texts obnubilated. The rear server can then come to a decision that records sq. Measure queried by way of the receiver making use of its personal key and conjointly the got internal checking out-states from the front server.

DES Algorithm:

- Step1: initial permutation
- Step 2: sixteen rounds approach
- Step 3: Left-right swap
- Step four: final permutation
- In an initial permutation, the bit values are swapped indiscriminately.
- The sixty-four-bit text splits into 2 thirty-two bit codecs known as left and correct.
- The combo of right thirty-two bit and key cost are passed as operate and XOR operation is made on handed function and left 32bit enter.
- The output of this XOR operation is that the output format of left 32bit.
- The left thirty-two bit is straight passed as an output of correct 32bit.
- Inside the operate the correct 32bit enter is distended to the forty-eight bit and forty-eight-bit key are processed to participate in XOR operation and likewise the effect's forty-eight-bit output.
- The forty-eight-bit structure is processed to perform S-box operation and compressed to the 32bit structure.
- In progress, the thirty-two-bit enter is cut up into four 8bit blocks every.
- Inside the output field, the blocks are divided into six blocks and each block occupies 8bit layout, for that reason completely forty-eight-bit output is made by using progress.
- In a while exploitation S-box operation it's compressed into thirty-two bit.
- In S-field operation the fundamental and last blocks are treated as rows and internal blocks are treated as columns.
- Exploitation the binary structure of row and column variety it can be searched in the matrix and also the cost of quantity is employed as binary layout and it's handled as output.

3.8 Module Description:

3.8.1 User module Description:

Share file: Used to transfer files into servers and wont to generate public key.

Send file: Used to test files that are sent among registered users.

Receive file: Used to test the received files among registered users.

Search file: With the assistance of public key it's wont to search the received files and request the server to come up with the keys.

Download file: Used to transfer the file with the assistance of 2 keys that are generated from twin server

3.8.2 Server1 Description:

File Details: Show the main points of sender, receiver and file details.

User Details: Show the main points of all registered users.

User Request: Consistent with the request of users the sever send the desired non-public keys to the mail of the receiver.

Download Details: Show details of all downloaded files by registered users

3.8.3 Server2 Description:

File Details: Show the main points of sender, receiver and file details.

User Details: Show the main points of all registered users.

User Request: Consistent with the request of users the sever send the desired non-public keys to the mail of the receiver.

Download Details: Show details of all downloaded files by registered users

3.8.4 Registration Description: Gets the main points of all users for registration of users.After completion of registration the user gets access to transfer files to servers and to send to registered users and additionally to receive files from registered users.

3.8.5 Architecture diagram:

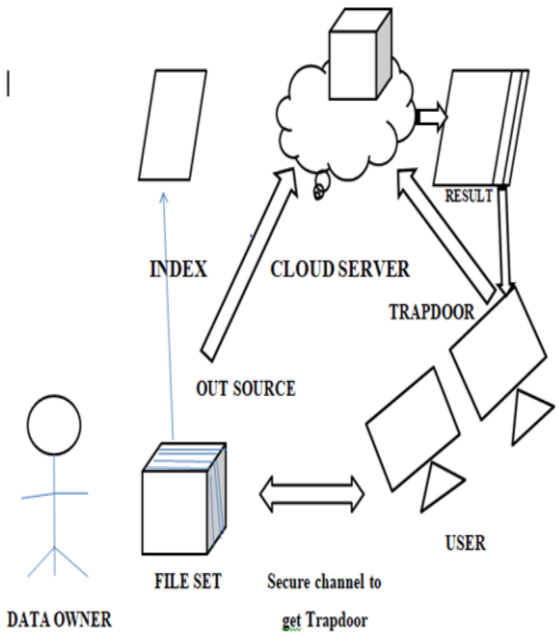

Figure.1: Architecture diagram

V. EXPERIMENTAL RESULTS

Home Page: The following figure shows the home page for the system. Its consists of navigation menu with options to user login, server 1 login, server 2 login and registration. User can use all the menu items available over the page.

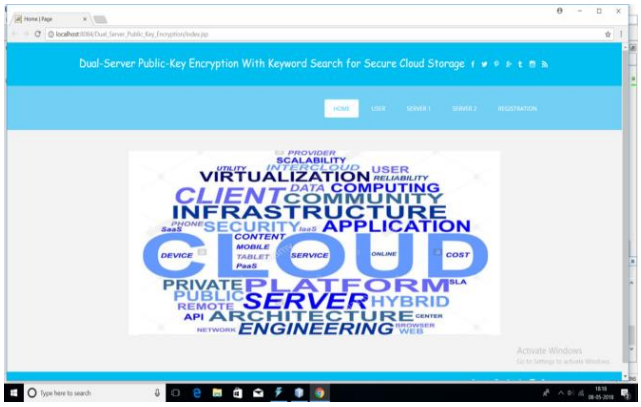

Fig.2 Home page

User Registration Page: The following figure 5.1.2 shows the User Registration Page. Here the user may able to register for the system by providing all necessary details like name, password and e-mail...etc. After entering all the details user must click on register then the registration has been done successfully.

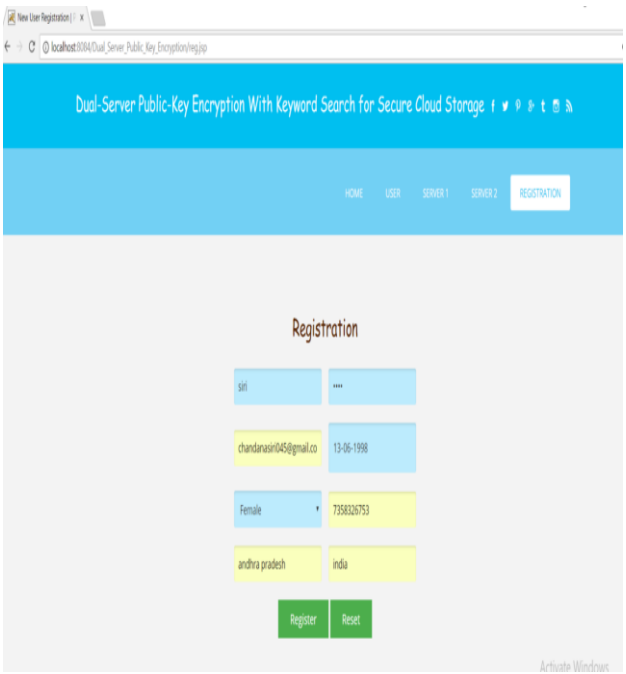

Fig. 3 Registration

User, server Login Page:

The following figure shows the User login Page. In this module user may login to the application. There must be two fields that are mandatory for the user to fill. They are (i) Username (ii) Password.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

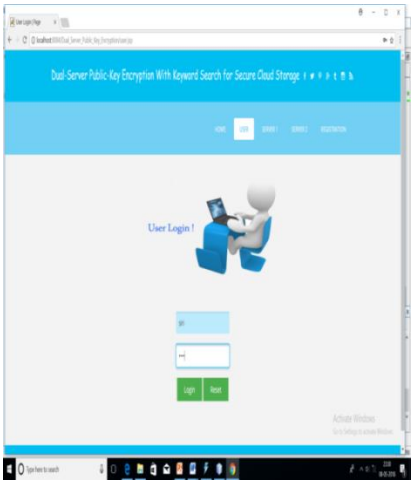

Fig.4 User login page

Upload page: User can share files to another user by generating public key. This file is then encrypted and stored in servers.

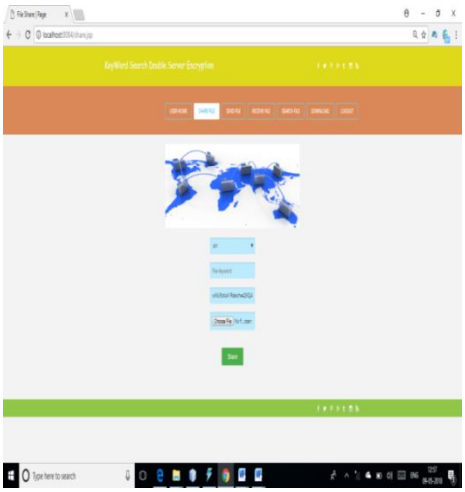

Fig 5 Upload Image

Keyword search page: User have to search the file using appropriate public key sent by sender.

Fig.6 Keyword search page

VI. CONCLUSION

On this paper, we tend to project a brand new process "keyword Search Double Server Encryption" so one can stop the inside keyword estimation assault that is an inherent vulnerability of the ordinary methodology. I conjointly used coding algorithms for encrypting and soft Projective Random function (SPRF) for key generation. SMTP and SSL are used for the cost-efficient switch of emails for causation keys. We have an inclination to planned a beginning constitution, elite Double Server Open Key secret writing with phrase Hunt (DS-PEKS), which will deter inside watchword estimate assault that is partner inborn best of the fine PEKS system. We have an inclination to all or any the equal given a rising glossy Projective Hash capability (SPHF) and used it to enhance a non-certain DS-PEKS plot. A productive intellectual object of the essential SPHF predicated on the Diffie-Hellman drawback is what's quite a lot of displayed at intervals the paper, that provides associate low in cost DS-PEKS conspire whereas no longer pairings. To raised assurance understanding security, this paper makes the important exercise to formally handle the topic of tedious for taking part in twin Server operations.

REFERENCES

1. Rongmao Chen, Yi Mu, Senior Member, IEEE, Guomin Yang, Member, IEEE, Fuchun Guo, and Xiaofen Wang" Dual-Server Public-Key Encryption With Keyword Search for Secure Cloud Storage" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 4, APRIL 2016
2. 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.
3. 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.
4. 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.
5. M. Bellare, A. Desai, E. Jokipii, and P. Rogaway. A concrete security treatment of symmetric encryption Analysis of the des modes of operation. In Proceedings of the 38th Annual Symposium on Foundations of Computer Science. IEEE, 1997.
6. Dawn Xiaodong Song David Wagner Adrian Perrig"Practical Techniques for Searches on Encrypted Data"fdawnsong, daw, perrigg@cs.berkeley.edu University of California, Berkeley
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. 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.
9. R. Gennaro and Y. Lindell, "A framework for password-based authenticated key exchange," in Proc. Int. Conf. EUROCRYPT, 2003, pp. 524-543.
10. 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.