A Review of Research on Dual -Server Public-Key Encryption with Keyword Search for Secure Cloud Storage

Shaikh Tofik S.[1], Gule Sheetal J.[2]

[1]Student, Computer Department, PREC Loni, Maharashtra, India
[2] Assistant Proffesor, Computer Department, PREC Loni, Maharashtra, India

ABSTRACT

Now a day's there will be growing popularity of cloud computing, large number of users and data owners are motivated to outsource their data to cloud servers for large convenience and reduced cost required for data management. However, important data should be encrypted before outsourcing for privacy requirements, which uses data utilization technique like keyword-based document retrieval. Searchable encryption is of expanding enthusiasm for ensuring the information protection in secure searchable distributed storage. In this paper, we research the security of a notable cryptographic primitive, in particular, public key encryption with keyword search (PEKS) which is exceptionally valuable in numerous utilizations of cloud storage. The conventional PEKS structure experiences an inalienable instability called inside Brut force keyword guessing attack propelled by the pernicious server. To address this security defenselessness, we propose another PEKS system named double server PEKS (DS-PEKS). As another principle commitment, we characterize another variation of the smooth projective hash capacities (SPHFs) alluded to as direct and homomorphic SPHF (LH-SPHF). We then demonstrate a bland development of secure DS-PEKS from LH-SPHF. To outline the plausibility of our new structure, we proposed system which makes system easy to handle and effective mechanism to handle complex task with better result with dual server public key encryption of the proposed scheme.

Keyword - *encryption, decryption, dual server encryption, cloud computing.*

1. INTRODUCTION

With the fast improvement of distributed computing and portable systems administration innovations, clients tend to get to their put away information from the remote distributed storage with cell phones. The fundamental favorable position of distributed storage is its pervasive client availability furthermore its for all intents and purposes boundless information stockpiling capacities. Notwithstanding such advantages gave by the cloud, the real test that remaining parts is the worry over the secrecy and protection of information while embracing the distributed storage administrations [1]. For example, decoded client information put away at the remote cloud server can be defenseless against outer assaults started by unapproved outcasts and inside assaults started by the dishonest cloud service provider (CSPs) organizations [2]. There are a few reports that affirm information breaks identified with cloud servers, because of malignant assault, burglary or inward mistakes [3]. This raises sympathy information may contain extremely delicate individual association/data.

Distributed cloud storage outsourcing has turned into a prominent application for undertakings and associations to lessen the weight of keeping up enormous information lately.No withstanding,
in all actuality, end clients may not by any means believe the cloud capacity servers and may want to scramble their information some time recently transferring them to the cloud server with a specific end goal to secure the information protection. This normally makes the information usage more troublesome than the conventional storage where information is kept in the nonappearance of encryption. One of the average arrangements is the searchable encryption which permits the client to recover

the scrambled records that contain the client indicated catchphrases, where given the watchword trapdoor, the server can discover the information required by the client without any problem .

1.1 PROBLEM STATEMENT

The Problem is to determine how to securely search any document from cloud in form of encrypted data with the help of dual servers.

- Dual Server-public key encryption with keyword search (PEKS).
- How to Store data in Secure form on cloud.
- How to Store data in Secure form on cloud.

2. LITERATURE SURVEY

Cloud computing represents today's most exciting computing pattern shift in information technology[1]. but, security and privacy are perceived as primary obstacles to its large adoption[2]. Here, outline several critical security challenges and motivate further investigation of security solutions for a trustworthy public cloud environment[3]. 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 stockpiling server play out the inquiry and answer the question without loss of information secrecy[4].

the issue of seeking on information that is encoded utilizing an 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[5].

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 Boneh et 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 et al., 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 ciphertext assault, and against watchword speculating assaults, despite the fact that these thoughts appear to be the most pragmatic use of PEKS primitives[6].

Aanother 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 ciphertext indistinguishability'[7].

3. EXISTING SYSTEM

In a PEKS framework, utilizing the recipient's open key, the sender connects some scrambled catchphrases (alluded to as PEKS ciphertexts) with the encoded information. The recipient then sends the trapdoor of a to-be-hunt catchphrase to the server down information seeking. Given the trapdoor and the PEKS ciphertext, the server can test whether the watchword hidden the PEKS ciphertxt is equivalent to the one chose by the recipient. Provided that this is true, the server sends the coordinating encoded information to the beneficiary.

Baek et al. proposed an ew PEKS conspire without requiring a protected channel, which is alluded to as a safe sans channel PEKS (SCF-PEKS).

Rhee et al. later improved Baek et al's. security display for SCF-PEKS where the assailant is permitted to acquire the relationship between the non-challenge ciphertexts and the trapdoor.

Byun et al.introduced the disconnected watchword speculating assault against PEKS as catchphrases are looked over a much littler space than passwords and clients typically utilize surely understood watchwords for seeking archives.

3.1 LIMITATIONS OF EXISTING SYSTEM:

Despite of being free from mystery key appropriation, PEKS plans experience the ill effects of an intrinsic weakness in regards to the trapdoor catchphrase security, in particular inside Keyword Guessing Attack (KGA). The reason prompting to such a security powerlessness is, to the point that any individual who knows collector's open key can produce the PEKS ciphertext of self-assertive watchword himself.

Specifically, given a trapdoor, the antagonistic server can pick a speculating watchword from the catchphrase space and after that utilization the watchword to produce a PEKS ciphertext. The server then can test whether the speculating catchphrase is the one fundamental the trapdoor. This speculating then-testing methodology can be rehashed until the right catchphrase is found.

On one hand, despite the fact that the server can't precisely figure the catchphrase, it is still ready to know which little set the basic watchword has a place with and in this way the watchword protection is not very much safeguarded from the server. Then again, their plan is unfeasible as the collector needs to locally locate the coordinating ciphertext by utilizing the correct trapdoor to sift through the non-coordinating ones from the set came back from the server.

4. PROPOSED SYSTEM

The commitments of this paper are depending on four-steps.

1] We formalize another PEKS system named Dual-Server Public Key Encryption with Keyword Search (DS-PEKS) to address the security defenselessness of PEKS.

2] A new variation of Smooth Projective Hash Function (SPHF), alluded to as direct and homomorphic SPHF, is presented for a nonexclusive development of DS-PEKS.

3] We demonstrate a non specific development of DS-PEKS utilizing the proposed Lin-Hom SPHF.

4] To delineate the possibility of our new system, a proficient instantiation of our SPHF in view of the Diffie-Hellman dialect is displayed in this paper.

4.1 ADVANTAGES OF PROPOSED SYSTEM

All the current plans require the blending calculation amid the era of PEKS ciphertext and testing and thus are less proficient than our plan, which does not require any matching calculation.

Our plan is the most productive as far as PEKS calculation. It is on account of that our plan does exclude matching calculation. Especially, the current plan requires the most calculation cost because of 2 blending calculation for each PEKS era.

In our proposed system, in spite of the fact that we additionally require another phase for the testing, our calculation cost is really lower than that of any current plan as we don't require any matching calculation and all the seeking work is taken care of by the server.

5 SYSTEM ARCHITECTURE

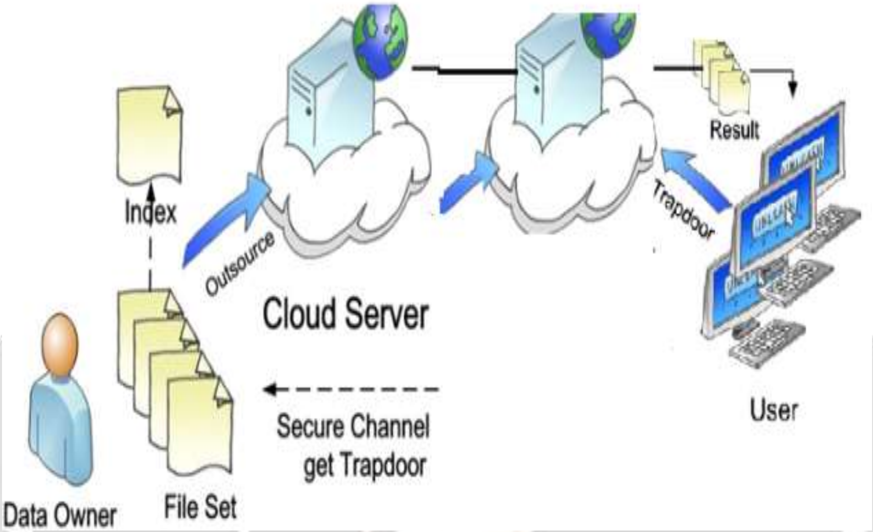

Fig -1 Dual server Architecture

5.1Data Owner :

Register with cloud server and login(username must be unique). Send request to Public key generator (PKG) to generate Key on the user name. Browse file and request Public key to encrypt the data, Upload data to cloud service provider. Verify the data from the cloud .

5.2 Public Key Generator :

Receive request from the users to generate the key, Store all keys based on the user names. Check the username and provide the private key. Revoke the end user (File Receiver if they try to hack file in the cloud server and un revoke the user after updating the private key for the corresponding file based on the user).

5.3 Key Update :

Receive all files from the data owner and store all files. Check the data integrity in the cloud and inform to end user about the data integrity. Send request to PKG to Update the private key of the user based on the date parameter (Give some date to update Private Key). List all files, List all updated Private Key details based on the date and users, List all File attackers and File Receive Attackers.

5.4 ALGORITHM

A DS-PEKS scheme is defined by the following algorithms.

_ Setup(1_). Takes as input the security parameter _, 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; pkFS; pkBS; kw1): Takes as input P, the front server's public key pkFS, the back server's public key

pkBS and the keyword kw1, outputs the PEKS ciphertext
CTkw1 of kw1;

_ DS-Trapdoor(P; pkFS; pkBS; kw2): Takes as input P,
the front server's public key pkFS, the back server's public
key pkBS and the keyword kw2, outputs the trapdoor

Tkw2 ;
_ FrontTest(P; skFS;CTkw1 ; Tkw2): Takes as input P,
the front server's secret key skFS, the PEKS ciphertext

CTkw1 and the trapdoor Tkw2 , outputs the internal testing-state CITS;

_ BackTest(P; skBS;CITS): Takes as input P, the back server's secret key skBS and the internal testing-state CITS, outputs the testing result 0 or 1;

6. RESULT AND DISCUSSION

Our proposed system gives a tremendous improvement than conventional system also shown that it is valuable in various digital data storage fields, which show a higher level of security,efficiency and scalability of the system. Proposed system satisfies the usability factor
like Satisfaction, accuracy, effectiveness and efficiency.
Also proposed system is robust, but also it gives better security mechanism than conventional system.

7. CONCLUSION

The Existing techniques on keyword-based encryption, which are widely used on the plaintext data, cannot be directly applied on the encrypted data. Downloading all the data from the cloud and decrypt locally is obviously impractical.

In this paper, we proposed another structure, named Dual- Server Public Key Encryption with Keyword Search (DSPEKS), that can keep within brutforce keyward attack which is an innate weakness of the PEKS system.
In future , According to technical view our proposed system is efficient and cost effective.

8. REFERENCES

1. Kamara S, Lauter K (2010) Cryptographic cloud storage. In: Sion R, Curtmola R, Dietrich S, Kiayias A, Miret JM, Sako K, Sebé F (eds) Financial Cryptography and Data Security, LNCS 6054. Springer, Berlin, Heidelberg, pp 136–149.

2. Hacigümüş H, Iyer B, Li C, Mehrotra S (2002) Executing sql over encrypted data in the database-service-provider model. In: Proceedings of SIGMOD, ACM, pp 216–227.

3. Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl 34:1–11.

4. 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.

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

6. L. Fang,W. Susilo, C. Ge, and J.Wang, “Public key encryption with keyword search secure against keyword guessing attacks without random oracle,” Inf. Sci., vol. 238, pp. 221–241, 2013.

7. 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**.**