Secure and Efficient Keyword Search in Multiple Cloud Servers with Using PKE & SSE

[1]Nagarapu Urmila, [2]P.Prashanth Kumar, [3]A.Ravi Kumar
[1]M. Tech Student, [2]Assistant Professor, [3]Associate Professor & HOD
[1]Department of CSE, Hyderabad, Telangana, India, [2]Department of CSE, Hyderabad, Telangana, India , [3]Department of CSE, Hyderabad, Telangana, India.

***ABSTRACT*–** we explore the security of an outstanding cryptographic primitive, in particular Public Key Encryption with Keyword Search which is exceptionally valuable in numerous uses of distributed storage. Unfortunately, it has been demonstrated that the normal PEKS structure experiences a natural weakness called inside Keyword Guessing Attack forced by the harmful server. Distributed computing, huge scope of clients and measurements administrators are affected to outsource their realities to cloud servers for enormous accommodation and diminished cost required for data administration. In any case, vital actualities should be scrambled sooner than outsourcing for security necessities, which utilizes records use method like catchphrase fundamentally, based record recovery. Accessible encryption is of expanding excitement for ensuring the information insurance in quiet accessible circulated carport. In this paper, we thinks about the security of a remarkable cryptographic primitive, especially, Public Key Encryption with Keyword Search (PEKS) that is very profitable in a few usages of distributed storage. The customary PEKS structure reports an unavoidable precariousness known as inside Brute Force catchword guesses attack moved through the cruel server. To address this security helplessness, we recommend some other PEKS framework named Dual Server PEKS (DS-PEKS). Through this propose framework, we can enhance the security for distributed storage frameworks.

1. INTRODUCTION

Cryptography is the act of changing information to make it garbled by an outsider, unless a specific bit of mystery data is made accessible to them. A wide range of types of cryptographic calculations exist, each intended for an alternate reason. An option is open key cryptography, which is regularly used to send messages to other individuals.

The present mail servers, for example, IMAP servers, record servers and other information stockpiling servers commonly should be completely believed—they approach the information, and henceforth should be trusted not to uncover it without approval—which presents bothersome security and protection chances in applications. Past work demonstrates to fabricate scrambled record frameworks and secure mail servers, however commonly one must give up usefulness to guarantee security. The fundamental emergency is that moving the calculation to the information storing looks excessively troublesome when the information is encoded, and in addition numerous calculation issues over scrambled information already had no pragmatic arrangements. With the quick change of circulated registering and versatile frameworks organization developments, customers have a tendency to get to their set away data from the remote dispersed stockpiling with PDAs. The basic great position of disseminated stockpiling is its unavoidable customer accessibility moreover it's in every way that really matters endless data accumulating limits. Despite such points of interest gave by the cloud, the genuine test that outstanding parts is the stress over the mystery and security of data while grasping the circulated stockpiling organizations.

For instance, decoded customer data set away at the remote cloud server can be vulnerable against external attacks began by unapproved outsiders and inside strikes began by the untrustworthy cloud specialist co-op (CSPs) associations. There are a couple of reports that certify data breaks related to cloud servers, in light of threatening attack, thievery or internal mix-ups. This raises sensitivity data may contain greatly fragile individual affiliation/information. Conveyed distributed storage outsourcing has turned out to be remarkable programming for endeavors and organizations to decrease the weight of keeping up enormous data as of late. No withstanding, in all reality, stop customers won't with the guide of any approach consider the cloud capacity servers and can need to scramble their data sometime of late moving them to the cloud server with a specific stop intend to agreeable the insights security. This ordinarily makes the insights usage harder than the conventional stockpiling where measurements are kept inside the nonappearance of encryption. One of the normal courses of action is the accessible encryption which lets in the supporter to recuperate the mixed records that include the buyer showed catchphrases, wherein given the watchword trapdoor, the server can find the data required by the customer with none issue.

2. RELATED WORK

R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky returned to the issue of accessible symmetric encryption, which enables a client to store its measurements on a faraway server in one of thusly that it might look for over it in a private way. We make various commitments which incorporate new wellbeing definitions and new structures. Persuaded by utilizing unpretentious issues in all past security definitions for SSE, we advocate new definitions and bring up that the current thoughts have sizable sensible disadvantages: in spite of the normal utilization of accessible encryption, they best certification security for clients that complete all their inquiries immediately. We address this issue through presenting more grounded definitions that assurance insurance regardless of the possibility that clients complete additional commonsense inquiries.

We additionally prompt two new SSE structures. Shockingly, paying little respect to being provably secure underneath this more grounded wellbeing definitions, these are the most effective plans up to now and are (asymptotically) first (i.e., the outline completed by utilizing the server in venture with again report is consistent inside the span of the realities). The principal motivation behind Dalia Khader considers move toward becoming to have a PEKS this is calm underneath a favored form set up of the irregular prophet show best. To achieve that, stage one transformed into finding an IBE plot that has key protection thoughts. Utilization of IBE with Weil matching to assemble a PEKS end up plainly exhibited and the plan end up noticeably comfortable under an assigned watchword strike however underneath the arbitrary prophet best. The IBE forewarned by Boneh and Boyenin furthermore transformed into no longer valuable in building a PEKS as demonstrated. It was enticing to endeavor to demonstrate the K-strong IBE to have a conviction of key security since it transformed into demonstrated that the Cramer-Shoup encryption is agreeable. The KRIBE took after an assortment of procedures from this encryption plan and KRIBE changed into turned out to be quiet. The new PEKS conspire changed into then used to gather an open key encryption with conjunctive watchword look and an open key encryption that does not require a protected channel. Be that as it may, the shiny new PEKS conspire still has a few disadvantages in light of the limitations of the KRIBE plot itself, in which the assortment of malignant clients is constrained to a couple of cost K. That is the scope of trapdoors produced inside the PEKS is controlled to at generally K. By the by, that isn't an extreme inconvenience where we should utilize a sensibly huge K for email looking projects. J. Baek, R. Safavi-Naini, and W. Susilo said three inconveniences related with PEKS and proposed provably secure PEKS plans that wipe out comfortable channel and encode a few watchwords productively. An exciting open issue is to plan a PEKS conspire in view of a primitive beside the BDH inconvenience.

A Public key encryption with catchphrase look returned to ", It suggests that The principal PEKS plot requires a secured channel to transmit the trapdoors. To beat this requirement, Author's proposed another PEKS plot without requiring a sheltered channel, which is implied as a safe sans channel PEKS (SCF-PEKS). The musing is to incorporate the server's open/private key consolidate into a PEKS system. The catchphrase figure substance and trapdoor are created using the server's open key and therefore simply the server (doled out analyzer) can play out the interest. New PEKS plot indicated as SCF-PEKS don't requires a secured channel to transmit trapdoor as in regular PEKS.In this Mentioned plan the aggressor is allowed to get the connection between the nonchallenge figure works and the trapdoor. Outside enemies can get the trapdoors sent in an open channel can reveal the encoded watchwords through detached catchphrase guessing attacks and they can perform disengaged watchword guessing attacks against the said (SCF-PEKS) plans.

R. Cramer and V. Shoup et al., "A Universal hash proofs and a worldview for versatile picked ciphertext secure open key encryption" In this paper Authors proposes smooth projective hash work (SPHF). Many arrangement in composing ends up being powerful against adaptable Chosen figure content attack however every one of them require a trusted outcast commitment amid the time spent customer enlistment for both sender and beneficiary. Makers at that point propose a rational scheme that can be shown secure against flexible picked figure content ambush under a sensible tenacity supposition is smooth projective hash work (SPHF) that of Cramer and Shoup . This arrangement relies upon Parlier's Decision Composite Residuosity (DCR) doubt [P], while another is arranged in the set up Quadratic Residuosity (QR) assumption.

3. FRAMEWORK

Public Key Encryption with Keyword Search (PEKS) that empowers a client to look encoded information in the asymmetric encryption setting. In a PEKS framework, utilizing the recipient's open key, the sender connects some scrambled catchphrases (alluded to as PEKS figure writings) with the encoded information. The recipient at that point sends the trapdoor of a to-be-looked watchword to the server for information seeking. Given the trapdoor and the PEKS figure message, the server can test whether the watchword fundamental the PEKS figure content is equivalent to the one chose by the beneficiary. Assuming this is the case, the server sends the

coordinating scrambled information to the recipient.

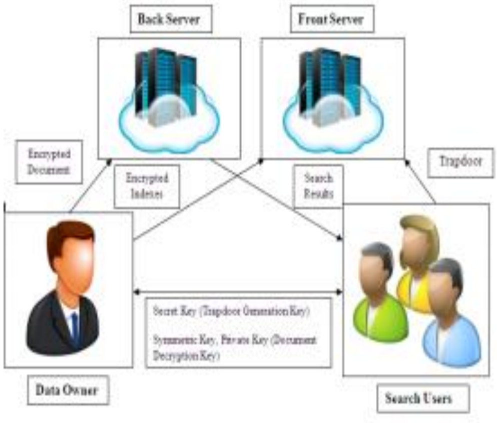


Figure 1. DS-PEKS System work flow

DS-PEKS conspire mostly comprises of (KeyGen, DS − PEKS, DS − Trapdoor, Front Test, Back Test). To be more exact, the KeyGen calculation produces general society/private key sets of the front and back servers rather than that of the collector. Besides, the trapdoor age calculation DS − the calculation Trapdoor takes as info the collector's private key. Such a distinction is because of the diverse structures utilized by the two frameworks. In the traditional PEKS, on the grounds that there is best one server, if the trapdoor age calculation is open, at that point the server can discharge a speculating assault against a watchword cipher text to show signs of improvement the scrambled catchphrase.

Be that as it may, underneath the DS-PEKS system, we can in any case accomplish semantic security while the trapdoor age calculation is open.

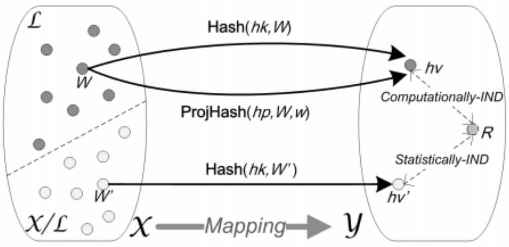
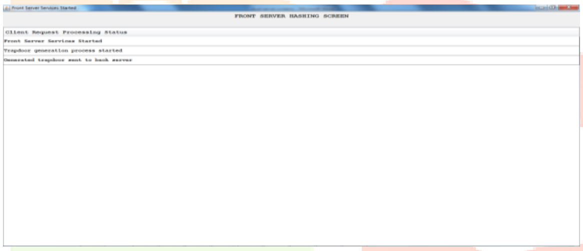


Figure 2. Smooth Projective Hash Function

Intuitively, this will be used as a sort of specified-verifier zero-information evidence (although it does no longer fulfill the classical 0-knowledge property): to prove the word belongs to language (*X€L*), the prove receives the projection key *hp* from the verifier, and hashes the word with admire to language, using *hp*, and sends again the end result. The verifier contrasts it to the hash attained with the secret key as well as accepts the proof if both hashes are the identical.

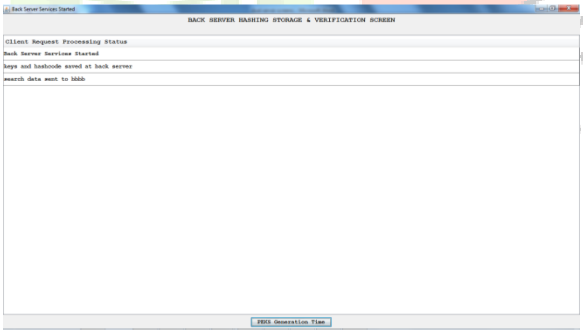
4. EXPERIMENT RESULTS

Our proposed framework gives a colossal change than regular framework additionally demonstrated that it is important in different computerized information stockpiling fields, which demonstrate a larger amount of security, efficiency and adaptability of the framework. Proposed framework fulfills the ease of use factor.



```
Front Server Services Started
FRONT SERVER HASHING SCREEN
Client Request Processing Status
Front Server Services Started
Trapdoor generation process started
Generated trapdoor sent to back server
```

Figure 3: Front Server



```
Back Server Services Started
BACK SERVER HASHING STORAGE & VERIFICATION SCREEN
Client Request Processing Status
Back Server Services Started
keys and hashcode saved at back server
search data sent to bbbb
```

Figure 4: Back Server

our plan is the most effective as far as PEKS calculation. It is on account of that our plan does exclude matching calculation. Especially, the plan requires the most calculation cost because of 2 blending calculation for every PEKS age. As for the trapdoor age demonstrated , as all the current plans don't include matching calculation, the calculation cost is much lower than that of PEKS age. As delineated in the plan cost the most time because of an extra matching calculation in the correct testing stage. One should take note of that this extra matching calculation is done on the client side rather than the server. In this way, it could be the calculation load for clients who may utilize a light gadget for seeking information. In our plan, 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 blending calculation and all the seeking work is taken care of by the server.

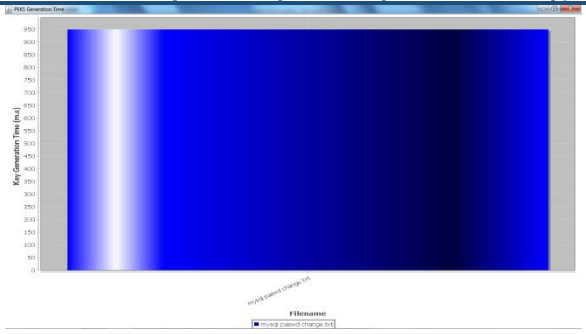


Figure 5: Key Generation time chart

5. CONCLUSION

In this paper, we proposed a new framework, Dual-Server Hybrid Key Encryption with Multi Keyword Search Scheme for secure cloud storage (DSPEKS), that can tackle the Query Complexity problem of existing DSPEKS framework. We also introduced a new Smooth Projective Hash Function (SPHF) and used it to construct a generic DSPEKS scheme. An efficient instantiation of the new SPHF based on the Diffie-Hellman problem is also presented in the paper, which gives an efficient DS-PEKS scheme without pairings

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, "Publickey 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: Consistencyproperties, relation to anonymous IBE, and extensions," in Proc. 25thAnnu. Int. Conf. CRYPTO, 2005, pp. 205–222.

[9] D. Khader, "Public key encryption with keyword search based onK-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.