International Journal of Cloud Computing and Database Management

**E-ISSN:** 2707-5915
**P-ISSN:** 2707-5907
IJCCDM 2020; 1(2): 01-03
Received: 18-01-2020
Accepted: 20-02-2020

**Maddela Sravanth Kumar**
Department of Computer Science, Sri Venkateswara University, Tirupati, Andhra Pradesh, India

**Corresponding Author:**
**Maddela Sravanth Kumar**
Department of Computer Science, Sri Venkateswara University, Tirupati, Andhra Pradesh, India

# A review on keyword search for secure cloud storage with multi-server public key encryption

**Maddela Sravanth Kumar**

**DOI:** https://doi.org/10.33545/27075907.2020.v1.i2a.10

**Abstract**
Searchable encryption is increasing interest for protecting the data privacy in secure searchable cloud storage. The security of a well-known cryptographic primitive, namely, public key encryption with keyword search (PEKS) which is very useful in many applications of cloud storage. Shockingly, it has been demonstrated that the customary PEKS structure experiences an inborn uncertainty called inside catchphrase speculating assault (KGA) propelled by the vindictive server. To address this security helplessness, to manage this security shortcoming, we will in general propose a being born PEKS framework named twofold server PEKS (DS-PEKS). As another rule responsibility, we will in general portray a beginning variety of the agile projective hash limits (SPHFs) insinuated as immediate and Homomorphic SPHF (LH-SPHF). We tend to around then show a dull advancement of secure DS-PEKS from LH-SPHF. To stipulate the opportunity of our initial framework, we will in general offer a decent portrayal of the last structure from a determination Diffie–Hellman-predicated LH-SPHF and exhibit that it will achieve the lively protection from inside the KGA.

**Keywords:** Encryption, Security, Catchphrase, Uncertainty, Framework

## 1. Introduction

Appropriated stockpiling re-appropriating has become a generally known application for attempts and relationship to decrease the encumbrance of keeping up vastly enormous information as of now. Be that since it could, illogicality, finish customers may not in any way shape or form accept the appropriated stockpiling servers and should encode their information before moving them to the cloud server to safeguard the information security. This routinely makes the data utilize more strenuous than the conventional warehousing any place data is solid while not cryptography. One in all the runs of the factory courses of action is that the open cryptography that supports the client to recoup the encoded records that contain the utilizer-doled out catchphrases, any place given the watchword trapdoor, the server will find the information required by the client while not unscrambling. Open cryptography is regularly recognized in either reciprocally symmetric or lopsided cryptography setting. In Melodic union, *et al.* arranged shibboleth looks on figure content, kenned as Accessible reciprocally symmetric cryptography (SSE) and a short timeframe later some SSE plans were assumed for changes. Tho' SSE plans enjoy high viability, they ability the evil impacts of nonplused secret key scattering. Customers must be constrained to share riddle keys that are utilized for information cryptography securely. Else they're not ready to empower the disrupted information re-appropriated to the cloud. To see this drawback, Boneh *et al.* given an extra adaptable crude, to be explicit Open Key cryptography with Watchword Inquiry (PEKS) that enables Associate in nursing client to check encoded information inside the channel request cryptography setting. In an exceedingly PEKS structure, abuse the gatherer's open key, the sender includes some encoded watchwords (suggested as PEKS figure compositions) with the disrupted information. The gatherer around then sends the trapdoor of a to-be-analyzed shibboleth to the server for information testing. Given the trapdoor and in this way the PEKS figure message, the server will investigate whether the watchword fundamental the PEKS figure content is indistinctly like the one winnowed by the recipient. Giving this is regularly valid, the server sends the coordinative disordered information to the beneficiary.

## 2. Related Work

Characterization of PEKS is depicted dependent on their security. To formalized mysterious IBE (AIBE) and introduced a conventional development of accessible encryption from

AIBE. They likewise told the best way to move a various leveled IBE (HIBE) plot into an open key encryption with impermanent catchphrase search (PETKS) where the trapdoor is just legitimate in a particular time interim. To show that the PEKS plans dependent on bilinear guide could be applied to assemble encoded and accessible inspecting logs. In order construct a PEKS secure in the standard model, we proposed a plan dependent on the k-flexible IBE and furthermore gave a development supporting different watchword search. The first PEKS plot without pairings. Secure Channel Free PEKS: The first PEKS plot requires a protected channel to transmit the trapdoors. To beat this restriction, proposed another PEKS plot without requiring a protected channel, which is alluded to as a safe san channel PEKS (SCF-PEKS). The thought is to include the server's open/private key pair into PEKS framework. The watchword figure content and trapdoor are created utilizing the server's open key and consequently just the server (assigned analyzer) can play out the hunt. SCF-PEKS where the assailant is permitted to get the connection between the non-challenge figure writings and the trapdoor. They additionally introduced a SCF-PEKS plot secure under the improved security model in the random. We presented the disconnected catchphrase speculating assault against PEKS as watchwords are looked over a lot littler space than passwords and clients as a rule utilize notable watchwords for looking through reports. They additionally called attention to that the plan was powerless to catchphrase speculating assault exhibited that outside foes that catch the trapdoors sent in an open channel can uncover the scrambled watchwords through disconnected catchphrase speculating assaults and they so flaunted line catchphrase speculating assaults against the CF- PEKS plans. The first PEKS conspire secure against outside watchword speculating assaults was proposed, the thought of trapdoor was proposed and there is an adequate condition for forestalling outside catchphrase speculating assaults. We proposed a solid SCF-PEKS conspire with (outside) KGA versatility. They likewise considered the versatile test prophet in their proposed security definition.

## 3. Usage

### 3.1 Smooth Projective Hash Functions (SPHFs):

In a general sense, SPHFs are groups of sets of limits (Hash, ProjHash) described on a figure of speech L. These limits are recorded by a burden of associated keys (hk, hp), where hk, the hashing key, are frequently optically perceived in light of the fact that the non-open key and drive, the projection key, on the grounds that everybody key. On a word W ∈ L, every limit should incite indistinctly proportional result: Hash (hk, L, W) with the hashing key and ProjHash (hp, L, W, w) with the projection key essentially in any case in any case an observer w that W ∈ L. Clearly, if W 6∈ L, such an observer doesn't exist, and along these lines the smoothness property communicates that Hash (hk, L, W) is liberated from strength. As Associate in the nursing result, be that as it may, the interesting expression strength, one can't figure Hash (hk, L, W).

### 3.2 Data Owner

It has the sizably voluminous data required to be hung on and shared inside the cloud framework. In our topic, the substance is to be faulted of forming File catchphrases and execution document write activity. What's more, it transfers ciphertext to cloud likewise watchwords (kw) are send to Servers. These 2 servers will engrave the watchwords and store inside the cloud.

### 3.3 Data User:

It needs to get to a gigantic assortment of information in the cloud framework. The element beginning downloads the comparing ciphertext. At that point it

**DS − Trapdoor (P, pkF S, pkBS, kw2):** Takes as info P, the front server's open key pkF S, the back server's open key pkBS and in this way the watchword kw2, yields the trapdoor Tkw2;

**FrontTest (P, skF S, CTkw1, Tkw2):** Takes as info P, the front server's mystery key skF S, the PEKS ciphertext CTkw1 and in this manner the trapdoor Tkw2, yields the inside testing-state CI T S;

**BackTest (P, skBS, CI T S):** Takes as information P, the back-server's mystery key skBS and consequently the inner testing-state CI T S, yields testing result zero or 1;

### iii) Front Server

Subsequent to accepting the question from the beneficiary, the front server pre-forms the trapdoor and all the PEKS ciphertexts utilizing its private key, and afterward sends some inward testing-states to the back server with the comparing trapdoor and PEKS ciphertexts covered up.

### iv) Back Server

Right now, back server would then be able to choose which reports are questioned by the recipient utilizing its private key and the got inward testing-states from the front server.

## 4. Results

Execution is assessed by making the examination between existing plans and our plan regarding calculation, size and security. All the current framework requires the blending calculation during the age of PEKS figure content and testing. Henceforth, these plans are less productive than our plan. Since our technique needn't bother with any matching calculation. In our plan, the calculation cost of PEKS age and testing are determined.

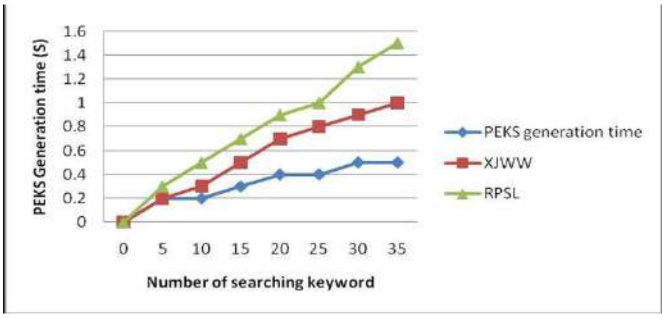

**Fig 1:** Number of searching keyword

When the searching keyword number is 30, the total computation cost of our scheme is about 0.5 seconds. As illustrated in Fig1, the scheme [10] cost the most time due to an additional pairing computation in the exact testing stage. One should note that this additional pairing computation done on the user side instead of the server. Therefore, it could be the computation burden for users who may use a light device for searching the data.

In our scheme, it also requires another stage for the testing but our computation cost is actually lower than that of any existing scheme. Our scheme does not require any pairing computation and all the searching work is handled by the server.

## 5. Conclusion

**I**n this paper, we proposed a new framework, named Dual-Server Public Key Encryption with Keyword Search (DS-PEKS), that can prevent the inside keyword guessing attack which is an inherent vulnerability of the traditional PEKS framework. We also introduced a new Smooth Projective Hash Function (SPHF) and used it to construct a generic DS-PEKS 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.

## 6. References

1. Chen R, Mu Y, Yang G, Guo F, Wang X. “A new general framework for secure public key encryption with keyword search,” in Proc. 20th Australasian Conf. Inf. Security Privacy (ACISP), 2015, 59-76.
2. Boneh D, Di Crescenzo G, Ostrovsky R, Persiano G. “Public key encryption with keyword search”, in Proc. Int. Conf. Advances in Cryptology -EUROCRYPT, 2004, 506-522.
3. Fang L, Susilo W, Ge C, Wang JA. “Secure channel free public key encryption with keyword search scheme without random oracle”, Cryptology and Network Security. 2009, 248-258.
4. Park, Dong Jin, Kihyun Kim, and PilJoong Lee, "Public Key Encryption with Conjunctive Field Keyword Search", 2004; 4:73-86.
5. Fang L, Susilo W, Ge C, Wang J. "Public key encryption with keyword search secure against keyword guessing attacks without random oracle." Information Sciences, 2013, 221-241.
6. Bellare M, Rogaway P. “Random oracles are practical: A paradigm for designing efficient protocols”, Proceedings of the 1st ACM conference on Computer and communications security, 1993, 62-73.
7. Canetti, Ran, OdedGoldreich, ShaiHalevi. “The random oracle methodology, revisited”, Journal of the ACM (JACM), 2004; 51(4):557-94.
8. Abdalla, Michel, *et al.* "Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions." in Proc. 25th Annu. Int. Conf. CRYPTO, 2005; 3621:205-222.
9. Khader D. “Public key encryption with keyword search based on K-resilient IBE”, in Proc. of Int. Conf. Comput. Sci. Appl. (ICCSA), 2006, 298-308.
10. Xu P, Jin H, Wu Q, Wang W. “Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack”, IEEE Trans. Comput., 2013; 62(11):2266-2277.
11. Di Crescenzo G, Saraswat V. “Public key encryption with searchable keywords based on Jacobi symbols”, in Proc. 8th Int. Conf. INDOCRYPT, 2007, 282-296.
12. Cocks, Clifford. “An identity-based encryption scheme based on quadratic residues”, in Cryptography and Coding. Cirencester, U.K.: Springer, 2001, 360-363.
13. Baek J, Safavi-Naini R, Susilo W. “Public key encryption with keyword search revisited”, in Proc. Int. Conf. Comput. Sci. Appl. (ICCSA), 2008, 1249–1259.
14. Rhee HS, Park JH, Susilo W, Lee DH. "Trapdoor security in a searchable public-key encryption scheme with a designated tester,” Journal of Systems and Software, 2010, 83.5, 763-771.