International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017), e-ISSN: 2455-2585
Volume 4, Issue 6, June-2018

PROTECTED CLOUD REPOSITORY WITH PUBLIC KEY SEARCH BY ENCRYPTION IN TWO SERVERS

[1]DUTHPHALA SATISH KUMAR, [2]A SANTHOSHI, [3]Dr. R CHINNAAPPALA NAIDU
[1]PG Scholar, Dept of CSE, St. Martin's Engineering College, Hyderabad, T.S, India
[2]Asst. Professor, Dept. of IT, St. Martin's Engineering College, Hyderabad, T.S, India
[3]Professor, Dept of CSE, St. Martin's Engineering College, Hyderabad, T.S, India

ABSTRACT

Searchable encryption is of increasing interest for shielding the information privacy in safe searchable cloud storage. In this paper, we check out the safety of a famous cryptographic primitive, specifically, public key encryption with key-word seeks (PEKS) which could be very beneficial in lots of programs of cloud storage. Unfortunately, it has been proven that the traditional PEKS framework suffers from an inherent lack of confidence referred to as interior keyword guessing attack (KGA) released via the malicious server. To cope with this protection vulnerability, we propose a new PEKS framework named twin-server PEKS (DS-PEKS). As any other main contribution, we outline a brand new variant of the clean projective hash capabilities (SPHFs) called linear and homomorphic SPHF (LH-SPHF). We then show an accepted creation of relaxed DS-PEKS from LH-SPHF. To illustrate the feasibility of our new framework, we offer a green instantiation of the general framework from a Decision Diffie–Hellman-based totally LH-SPHF and show that it could attain the sturdy protection towards within the KGA.

Index terms: Keyword search, secure cloud storage, encryption, inside keyword guessing attack, smooth projective hash function, Diffie-Hellman language.

I. INTRODUCTION

Cloud storage outsourcing has emerged as a popular utility for enterprises and agencies to reduce the burden of keeping massive records in recent years. However, in fact, quit customers may not entirely trust the cloud stirage servers and might prefer to encrypt their statistics before importing them to the cloud server with the intention to defend the statistics privateness. This typically makes the statistics usage more tough than the conventional garage in which records is stored within the absence of encryption. One of the standard answers is the searchable encryption [3] which permits the person to retrieve the encrypted documents that comprise the user-certain keywords, wherein given the key-word trapdoor, the server can find the records required by means of the consumer without decryption. Searchable encryption [2] may be found out in either symmetric or uneven encryption setting. Song et al. [4] Proposed keyword seek on ciphertext, referred to as Searchable Symmetric Encryption (SSE) and afterwards numerous SSE schemes have been designed for upgrades. Although SSE [4] schemes experience excessive performance, they are afflicted by complex mystery key distribution. Precisely, users have to securely proportion secret keys which are used for statistics encryption. Otherwise they are not capable of percentage the encrypted data outsourced to the cloud. To resolve this problem, Boneh et al brought a more flexible primitive, particularly Public Key Encryption [8] with Keyword Search (PEKS) that enables a user to search encrypted data inside the asymmetric encryption setting. In a PEKS system, the usage of the receiver's public key, the sender attaches a few encrypted keywords with the encrypted records. The receiver then sends the trapdoor of a to-be-searched keyword to the server for facts looking. Given the trapdoor and the PEKS ciphertext, the server can check whether the key-word underlying the PEKS ciphertxt is equal to the only decided on by way of the receiver. If so, the server sends the matching encrypted information to the receiver.

II. RELATED DATA

In this subsection, we describe a category of PEKS schemes based totally on their protection. Traditional PEKS: Following Boneh et al.'s seminal paintings, Abdalla et al formalized nameless IBE (AIBE) and provided a usual production of searchable encryption from AIBE. They additionally showed a way to switch a hierarchical IBE (HIBE) scheme into a public key encryption with temporary keyword search (PETKS) where the trapdoor is handiest valid in a specific time interval. Waters et al[2] confirmed that the PEKS schemes based totally on bilinear map can be applied to build encrypted and searchable auditing logs. In order to construct a PEKS relaxed in the popular model, In [3] Khader proposed a scheme primarily based on the okay-resilient IBE and also gave a construction supporting a couple of-keywords seek. The first PEKS scheme without pairings turned into brought by using Di Crescenzo and Saraswat. The creation is derived from Cock's IBE scheme which isn't always very practical. 2) Secure Channel Free PEKS [6] : The unique PEKS scheme requires a at ease channel to transmit the trapdoors. To overcome this dilemma, Baek et al proposed a new PEKS scheme without requiring a at ease channel, that is called a comfortable channel-unfastened PEKS (SCF-PEKS) [4]. The concept is to add the server's public/private key pair into a PEKS machine. The key-word ciphertext and trapdoor are generated using the server's public key and subsequently handiest the server (precise tester) is capable of perform the hunt. Rhee et al [7] later greater Baek et al.'s protection model for SCF-PEKS where the attacker is allowed to obtain the relationship between the non-mission ciphertexts and the trapdoor. They also offered an SCF-PEKS scheme secure below the improved security version inside the random oracle version. Another extension on SCF-PEKS is through Emura et al. They stronger the security version with the aid of introducing the adaptively comfortable SCF-PEKS, wherein an adversary is allowed to issue test queries adaptively.

III. IMPLEMENTED MODEL

Against Outside KGA: Byun et al brought the off-line keyword guessing attack towards PEKS as key phrases are selected from a much smaller space than passwords and customers normally use well-known keywords for searching documents. They also mentioned that the scheme proposed in [9] Boneh et al turned into vulnerable to key-word guessing assault. Inspired through the work of Byun et al Yau et al validated that out of doors adversaries that capture the trapdoors sent in a public channel can monitor the encrypted key phrases via off-line key-word guessing assaults and they also confirmed off-line key-word guessing assaults in opposition to the (SCF-)PEKS [11] schemes. The first PEKS scheme comfortable against outside key-word guessing attacks were proposed through Rhee et al. The notion of trapdoor indistinguishability becomes proposed and the authors confirmed that trapdoor indistinguishability is an enough circumstance for preventing outside key-word-guessing attacks. Fang et al proposed a concrete SCF-PEKS scheme with (outdoor) KGA resilience. Similar to this work, they also taken into consideration the adaptive take a look at oracle of their proposed protection definition.

Against Inside KGA: Nevertheless, all of the schemes mentioned above are located to be prone to key-word guessing assaults from a malicious server (i.e., interior KGA). Jeong et al showed a negative result that the consistency/correctness of PEKS [3] implies lack of confidence to internal KGA in PEKS. Their end result suggests that constructing cozy and consistent PEKS schemes towards internal KGA is not possible beneath the original framework. An ability answer is to advocate a new framework of PEKS. Peng et al. [11] proposed the perception of Public-key Encryption with Fuzzy Keyword Search (PEFKS) wherein each key-word corresponds to a specific trapdoor and a fuzzy trapdoor. The server is most effective supplied with the fuzzy trapdoor and therefore can now not research the precise keyword considering that or extra keywords proportion the same fuzzy keyword trapdoor. However, their scheme suffers from numerous obstacles regarding the safety and performance. On one hand, even though the server cannot exactly wager the key-word, it is still capable of recognize which small set the underlying key-word belongs to and as a consequence the key-word privacy is not properly preserved from the server. On the other hand, their scheme is impractical as the receiver has to domestically locate the matching ciphertext through the usage of the exact trapdoor to filter out the non-matching ones from the set returned from the server.

Differences among This Work and Its Preliminary Version [1]: Portions of the paintings presented on this paper have previously appeared as a prolonged summary. Compared to [1], we have revised and enriched the paintings substantially inside the following elements. First, in the initial work in which our standard DS-PEKS construction was supplied; we confirmed neither a concrete construction of the linear and homomorphic SPHF nor a sensible instantiation of the DS-PEKS [10] framework. To fill this hole and illustrate the feasibility of the framework, in this paper, we first show that a linear homomorphism language LDH can be derived from the Diffie-Hellman assumption and then assemble a concrete linear and homomorphism SPHF, known as SPHFDH, from LDH. We provide a proper proof that SPHFDH is correct, clean and pseudo-random and therefore can be used for the instantiation of our standard creation. We then present a concrete DS-PEKS scheme from SPHFDH. To analyze its performance, we first deliver a contrast between current schemes and our scheme and then evaluate its overall performance in experiments. We additionally revised the initial version to decorate the presentation and clarity. In the related work element, compared to the preliminary model, we add extra literatures and provide a clearer type of the prevailing schemes primarily based on their security. We gift the security models of DS-PESK as experiments to make them more readable. Moreover, to make the concepts of SPHF and our newly described variant clearer, we upload Fig. Four and Fig. Five to highlight their key houses.

IV. PROPOSED TECHNOLOGY

A DS-PEKS scheme especially includes KeyGen, DS-PEKS, DS-Trapdoor, Front Test, and BackTest. To be more precise, the KeyGen algorithm generates the public/ non-public key pairs of the back and front servers in place of that of the receiver. Moreover, the trapdoor era set of rules DS-Trapdoor defined right here is public while within the conventional PEKS definition, the set of rules Trapdoor takes as input the receiver's non-public key. Such a distinction is due to the distinct structures used by the 2 structures. In the traditional PEKS, when you consider that there may be only one server, if the trapdoor technology algorithm is public, then the server can launch a guessing attack towards a key-word ciphertext to get better the encrypted keyword. As an end result, it is not possible to reap the semantic protection as described. However, as we are able to display later, underneath the DS-PEKS framework, we are able to nevertheless acquire semantic protection whilst the trapdoor era set of rules is public. Another distinction between the conventional PEKS and our proposed DS-PEKS is that the check set of rules is divided into algorithms; Front Test and Backrest run by way of unbiased servers. This is important for reaching security against the inner keyword guessing attack. In the DS-PEKS machine, upon receiving a query from the receiver, the front server pre-procedures the trapdoor and all the PEKS ciphertexts using its personal key, after which sends a few inner trying out-states to the returned server with the corresponding trapdoor and PEKS ciphertexts hidden. The again server can then determine which documents are queried by using the receiver the usage of its non-public key and the acquired internal trying out-states from the front server.

Security Models: In this subsection, we formalise the subsequent safety fashions for a DS-PEKS scheme towards the adverse front and back servers, respectively. One should word that each the front server and the lower back server right here are supposed to be "honest however curious" and will not collude with each different. More exactly, each the servers carry out the testing strictly following the scheme processes but can be curious about the underlying key-word. We need to be aware that the subsequent safety models also suggest the security ensures towards the outside adversaries that have less functionality in comparison to the servers.

Adversarial Front Server: In this part, we outline the safety in opposition to an adversarial front server. We introduce games, particularly semantic-safety towards chosen key-word attack and indistinguishability in opposition to keyword guessing attack1 to seize the security of PEKS ciphertext and trapdoor, respectively.

Adversarial Back Server: The security models of SS-CKA and IND-KGA in phrases of an adverse lower back server are similar to the ones towards a hostile front server. III. Semantic-Security in opposition to Chosen Keyword Attack. Here the SS-CKA experiment in opposition to an adverse again server is similar to the one in opposition to a hostile the front server besides that the adversary is given the personal key of the back server rather than that of the front server. We omit the info right here for simplicity.

V. CONCLUSION

In this paper, we proposed a new framework, named Dual-Server Public Key Encryption with Keyword Search (DS-PEKS) that could save you the inner key-word guessing assault that is an inherent vulnerability of the traditional PEKS framework. We also delivered a brand new Smooth Projective Hash Function (SPHF) and used it to assemble a general DS-PEKS scheme. An efficient instantiation of the brand new SPHF based at the Diffie-Hellman hassle is likewise provided within the paper, which gives an efficient DS-PEKS scheme without pairings.

VI. REFERENCES

[1] 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.

[2] M. Abdalla *et al.*, "Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions," in *Proc. 25th Annu. Int. Conf. CRYPTO*, 2005, pp. 205–222.

[3] D. Khader, "Public key encryption with keyword search based on K-resilient IBE," in *Proc. Int. Conf. Comput. Sci. Appl. (ICCSA)*, 2006, pp. 298–308.

[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] G. Di Crescenzo and V. Saraswat, "Public key encryption with searchable keywords based on Jacobi symbols," in *Proc. 8th Int. Conf. INDOCRYPT*, 2007, pp. 282–296.

[6] C. Cocks, "An identity based encryption scheme based on quadratic residues," in *Cryptography and Coding*. Cirencester, U.K.: Springer, 2001, pp. 360–363.

[7] J. Baek, R. Safavi-Naini, and W. Susilo, "Public key encryption with keyword search revisited," in *Proc. Int. Conf. Comput. Sci. Appl. (ICCSA)*, 2008, pp. 1249–1259.

[8] H. S. Rhee, J. H. Park, W. Susilo, and D. H. Lee, "Improved searchable public key encryption with designated tester," in *Proc. 4th Int. Symp. ASIACCS*, 2009, pp. 376–379.

[9] K. Emura, A. Miyaji, M. S. Rahman, and K. Omote, "Generic constructions of secure-channel free searchable encryption with adaptive security," *Secur. Commun. Netw.* vol. 8, no. 8, pp. 1547–1560, 2015.

[10] J. W. Byun, H. S. Rhee, H.-A. Park, and D. H. Lee, "Off-line keyword guessing attacks on recent keyword search schemes over encrypted data," in *Proc. 3rd VLDB Workshop Secure Data Manage. (SDM)*, 2006, pp. 75–83.

[11] W.-C. Yau, S.-H. Heng and B.-M. Goi, "Off-line keyword guessing attacks on recent public key encryption with keyword search schemes," in *Proc. 5th Int. Conf. ATC*, 2008, pp. 100–105.

[12] J. Baek, R. Safavi-Naini, and W. Susilo, "On the integration of public key data encryption and public key encryption with keyword search," in *Proc. 9th Int. Conf. Inf. Secur. (ISC)*, 2006, pp. 217–232.