WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

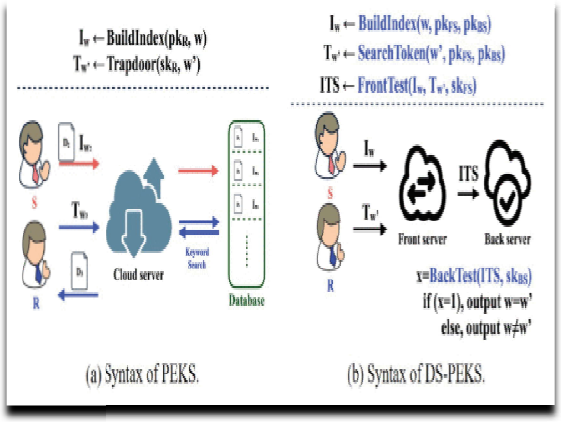
Multiple Server Data Encryption In Wireless Network

Prof. Gouri Patil , Mansee Pathak, Lisha J Patel, Mansi, Marshal Kevin

Guru Nanak Dev Engineering College Bidar

Introduction

Nowadays, the cloud services are ubiquitous in real-life. For example, people would like to outsource their photos to Google Drive for reducing cell-phone storage usage. If such data are confidential such as phone numbers, birthdays, credit card numbers or even medical records, it leads a serious security issue for secrecy and privacy. In fact, some financial service providers and on-line banks store extremely sensitive data like bank account numbers and credit card numbers from their consumers. In addition to the issue of authenticity which can be done by authentication schemes [1], [2], the security issue of the outsourced data has also been highly attracted attention along with the spread of cloud applications. A natural solution is directly to encrypt such confidential data before storing but we are not able to do any computation over these encrypted data. For general purposes, fully homomorphic encryption (FHE) firstly introduced by Gentry [3] is a very powerful tool to achieve the goal, but as we knew the computation cost of FHE is quite expansive. For specific purposes (i.e., searching, indexing, clustering, optimizing), we should have some more efficient solutions, and thus cryptosystems with extra specific functionalities [4] have been regarded as an urgent requirement in the modern technology. Searchable encryption is a cryptographic notion that allows servers to search over encrypted documents without losing their privacy. The first public key encryption with keyword search (abbreviated as PEKS) was proposed by Boneh et al. [5] in 2004. It works in the following scenario (illustrated in Fig. 1(a)): a sender encrypts a document and its searchable keyword using a receiver's public key. Then, the sender stores the document as well as the index (encrypted keyword) on a cloud data server. Once the receiver wants to retrieve her own documents (related to some keywords), she generates a trapdoor using her private key and the desired keyword. On receiving the trapdoor from the receiver, the cloud storage server executes tests between the input trapdoor and all index stored on the server. The corresponding documents will be returned when the keyword hidden in the index is verified equal to the keyword in the trapdoor. For simplicity, we usually focus on the 'keyword search' part, and omit the security of the encryption and decryption of documents. It is assumed that the encryption of documents is secure. PEKS immediately attracted lots of significant interests. Based on the notion of [5], numerous follow-up works have been proposed to achieve different requirements of keyword search. Boneh and Waters [6] proposed a PEKS construction about multi-keyword search, which is able to support conjunctive keyword search, subset keyword search and range queries. The conjunctive keyword search is widely discussed in [7], [8]. However, on considering the security of trapdoors [9], most PEKS schemes rely on a secure channel to secretly transfer the trapdoor. Baek et al. proposed a secure-channel free PEKS [10] solution to deal with this issue. Some PEKS surveys [10]–[12] aim to compare existing PEKS schemes and show some limitations in this area. An inherent limitation is the low-entropy of keywords. Byun et al. [13] introduced the off-line keyword guessing attacks which can be referred to as a kind of brute force attacks but is somehow realistic. More precisely, there is an adversary who is able to obtain the hidden keyword of index by testing one by one keyword in the dictionary. Some recent works (i.e., [14]–[16]) tackle the security against off-line keyword guessing attacks and some work for the version of certificateless keyword search [17]. A threat, called Inner Keyword Guessing Attacks [18], [19], is a new security issue about trapdoor privacy. On receiving a trapdoor from a receiver, a malicious server can easily obtain the hidden low-entropy keyword in the trapdoor by keeping making index with different keywords and then executing tests between the index and the trapdoor. This threat is different from the prior attacks as above, and particularly formalize weaknesses from the correlation between index and trapdoor.



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.

2.1 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.

Problem Statement

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

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

Proposed System

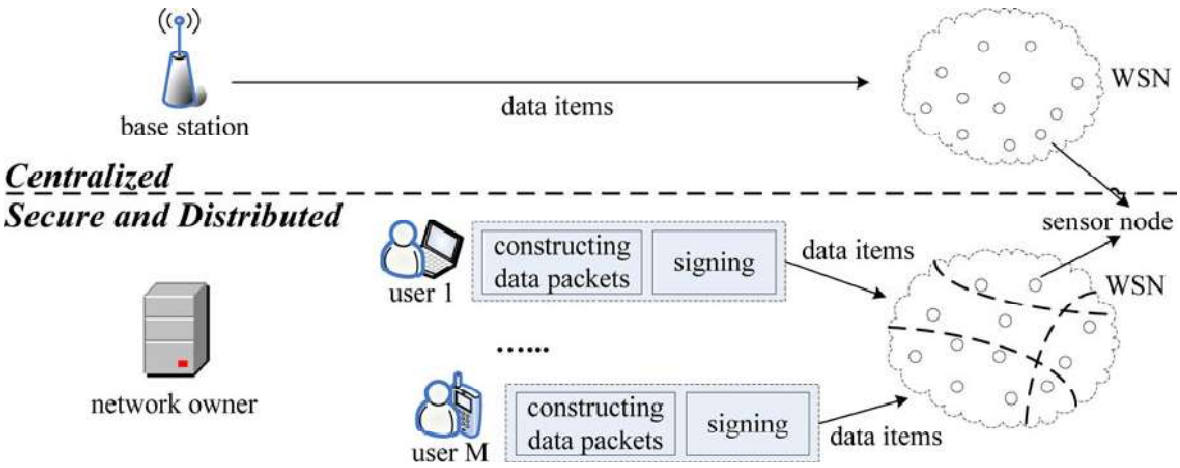
1. The commitments of this paper are depending on four-steps.
2. We formalize another PEKS system named Dual-Server Public Key Encryption with Keyword Search (DSPEKS) to address the security defenselessof PEKS.
3. A new variation of Smooth Projective Hash Function (SPHF), alluded to as direct and homomorphic SPHF, is presented for a nonexclusive development of DS-PEKS.
4. We demonstrate a non specific development of DS-PEKS utilizing the proposed Lin-Hom SPHF.
5. To delineate the possibility of our new system, a proficient instantiation of our SPHF in view of the DiffieHellman 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.

System Design



Methodology

- **Setting up Network Model**

System comprise of four stage, structure instatement, customer joining, parcel pre-handling and bundle check. For our fundamental protocol,in structure inauguration phase, the structure proprietor make its unlock plus confidential keys, plus afterward stacks the open parameter on top of every hub previous to the system organization. during the client combination stage, a client get the scattering benefit from side to side enrolling towards the system proprietor. In bundle pre-preparing phase, in the parcel confirmation phase, a hub checks each gotten bundle. In the event that the outcome is sure, it refreshes the information as indicated by the got parcel. In the accompanying, each stage is depicted in detail.

- **System Initialization Phase:**

In this stage, The system proprietor does the accompanying strides to determine private key plus a few open parameter. it at that point chooses the confidential key plus figures the open key. From that point onward, the open parameter be preloaded inside every hub of the system.

- **User Joining Phase:**

This stage be conjured at what timeclient through the character U-ID, plans towards get benefit stage. Client picks the confidential key and processes the open key. At that point client send a UID to the system proprietor, where Prij signifies the scattering benefit of client. After getting this message, the system proprietor produces the declaration.

- **Packet Pre-Processing Phase:**

Expect so as to a client, enter the WS-N plus needs to scatter n information things used for the development of the parcels of the individual information, we have two strategies.

- **Packet Verification Phase:**

Next towards the direct at what time a sensor hub, state, get a package also as ofapprove client or from its one-bounce neighbors, it primary check the packet's key ground. Looking at the two techniques, the information hash chain strategy brings about less correspondence transparency.

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 brutforcekeyward attack which is an innate weakness of the PEKS system. In future , According to technical view our proposed system is efficient and cost effective.

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.

References

1. C.-M. Chen, K.-H. Wang, K.-H. Yeh, B. Xiang, and T.-Y. Wu, ''Attacks and solutions on a three-party password-based authenticated key exchange protocol for wireless communications,'' J. Ambient Intell. Humanized Comput., vol. 10, no. 8, pp. 3133–3142, Aug. 2019.

2. C.-M. Chen, B. Xiang, Y. Liu, and K.-H. Wang, ‘‘A secure authentication protocol for Internet of vehicles,’’ IEEE Access, vol. 7, pp. 12047–12057, 2019.
3. C. Gentry, ‘‘Fully homomorphic encryption using ideal lattices,’’ in Proc. 41st Annu. ACM Symp. Theory Comput., v2009, pp. 169–178, doi: 10.1145/1536414.1536440.
4. D. Boneh, A. Raghunathan, and G. Segev, ‘‘Function-private subspacemembership encryption and its applications,’’ in Advances in Cryptology (ASIACRYPT) (Lecture Notes in Computer Science), vol. 8269. Berlin, Germany: Springer, 2013, pp. 255–275, doi: 10.1007/978-3-642-42033-7_14.
5. D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, ‘‘Public key encryption with keyword search,’’ in Advances in Cryptology (EUROCRYPT) (Lecture Notes in Computer Science), vol. 3027. Berlin, Germany: Springer, 2004, pp. 506–522.
6. D. Boneh and B. Waters, ‘‘Conjunctive, subset, and range queries on encrypted data,’’ in Proc. Theory Cryptogr. Conf. (Lecture Notes in Computer Science), vol. 4392. Berlin, Germany: Springer, 2007, pp. 535–554.