International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 07
March 2018

Public Key Encryption for Keyword Search in Cloud Using Kdm Security Scheme

Mr.J.Rajaram

Associate Professor

Rajaram.jatothu@gmail.com

R.MEDHA REDDY medhareddy96@gmail.com UG SCHOLAR

M.MAHESHKOUSHIK koushik8815@gmail.com UG SCHOLAR

K.SHARAN sharan.furious@gmail.com UG SCHOLAR

VIGNAN INSTITUTE OF TECHNOLOGY AND SCIENCE Vignan Hills, Near Ramojifilm city Deshmukhi (Village), Yadadri Bhuvanagiri Dist, Telangana– 508284

ABSTRACT:

Searchable encryption is of growing interest for protective the records privateness in secure searchable cloud storage. In this paper, we study the safety of a famous cryptographic primitive, in particular, public key encryption with key-word search (PEKS) which could be very useful in lots of applications of cloud garage. To address this safety vulnerability, we recommend a today's PEKS framework named dual-server PEKS (DS-PEKS).We present new frameworks for constructing public-key encryption schemes satisfying key-set up message (KDM) protection. We present new frameworks for building KDM-relaxed encryption schemes and twin mode cryptosystems that admit a very easy and modular assessment.

INTRODUCTION:

Cloud computing has appreciably impacted the computing infrastructure and enabled a large pool of packages. For example, statistics outsourcing [1] lets in small/medium period corporations to increase information availability with the beneficial aid of minimizing the manipulate and protection prices. Data outsourcing, however its merits, will growth huge records privacy issues for clients. Traditional encryption techniques may be used to triumph over such privateers concerns. However, famous encryption does now not allow seek capabilities on the encrypted statistics. Therefore, a big quantity of research is focused on Searchable Encryption (SE) era that can be used to efficaciously cope with this problem. There

are important branches of SE in which each is tailored for an amazing set of software program. Dynamic Searchable Symmetric Encryption (DSSE) (e.g., [2, 3, 4]) offers search abilities on encrypted information for private records outsourcing packages (e.g., data garage on the cloud), in which the client uses her very personal key to encrypt after which seek on her very personal statistics over the cloud. Public Key Encryption with Keyword Search (PEKS) schemes [5] allows any customer to encrypt information with certain key phrases under most of the people key of a designed receiver. The designed receiver, Alice, can then use her non-public key to generate and ship trapdoors for her favored key phrases, and permit the server to go looking at the encrypted information to retrieve the files which is probably associated with the key-word. PEKS is well acceptable for dispensed programs (e.g., email, audit logging for Internet of Things, and plenty of others.) wherein a large variety of users/entities generate encrypted facts to be retrieved through way of using a receiver. The attention of this paper is on PEKS schemes

2. LITERATURE SURVEY

1) A new standard framework for at ease public key encryption with keyword search

AUTHORS: R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang

Public Key Encryption with Keyword Search (PEKS), introduced through Boneh et al. In Eurocrypt'04, permits clients to look encrypted documents on an untrusted server without revealing any records. This perception may be very beneficial in lots of packages and has attracted a whole lot of attention by way of the usage of the cryptographic research network. However, one trouble of all the present PEKS schemes is they cannot face up to the Keyword Guessing Attack (KGA) launched with the aid of manner of a malicious server. In this paper, we suggest a present day PEKS framework named Dual-Server Public Key Encryption with Keyword Search (DSPEKS). This new framework can resist all of the assaults, together with the KGA from the two untrusted servers, so long as they do not collude. We then present a regular creation of DS-PEKS the use of a new edition of the Smooth Projective Hash Functions (SPHFs), this is of unbiased interest.

2) Searchable symmetric encryption: Improved definitions and efficient buildings

AUTHORS: R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky,

Searchable symmetric encryption (SSE) lets in a celebration to outsource the garage of his facts to each other birthday party in a personal way, even as maintaining the functionality to selectively searching for over it. This trouble has been the focal point of energetic studies and several safety definitions and homes were proposed. In this paper we begin with the aid of reviewing current notions of safety and recommend new and more potent safety definitions. We then present two constructions that we display at ease under our new definitions. Interestingly, similarly to pleasurable stronger protection guarantees, our homes are extra inexperienced than all previous buildings. Further, preceding paintings on SSE best taken into consideration the placing in which best the owner of the information is able to submitting seek queries. We do not forget the herbal extension where an arbitrary organization of occasions apart from the proprietor can put up search queries. We officially define SSE in this multi-consumer setting, and present an efficient production.

3) Public Key Encryption with Keyword Search based totally on K-Resilient IBE

AUTHORS: D. Khader

An encrypted e-mail is sent from Bob to Alice. A gateway wants to check whether or now not a certain key-word exists in an electronic mail or not for a few reason (e.g. Routing). Nevertheless Alice does now not need the email to be decrypted by using everybody besides her which includes the gateway itself. This is a situation wherein public key encryption with key-word are seeking (PEKS) is needed. In this paper we assemble a present day scheme (KR-PEKS) the Resilient Public Key Encryption with Keyword Search. The new scheme is comfortable beneath a designated key-phrase assault without the random oracle. The potential of building a Public Key Encryption with Keyword Search from an Identity Based Encryption modified into used in the introduction of the KR-PEKS. The safety of the brand new scheme was proved via way of displaying that the used IBE has a belief of key privacy. The scheme changed into then changed in wonderful methods so one can satisfy every of the

following: the first modification has become accomplished to enable multiple keyword searches and the alternative turned into completed to eliminate the need of at ease channels.

4) Generic buildings of comfortable-channel unfastened searchable encryption with adaptive safety

AUTHORS: K. Elmira, A. Miyaji, M. S. Rahman, and K. Omote,

For searching keywords towards encrypted information, public key encryption scheme with keyword search (PEKS), and its extension secure-channel free PEKS (SCF-PEKS), has been proposed. In this paper, we boom the safety of SCF-PEKS, calling it adaptive SCF-PEKS, wherein an adversary (modeled as a "malicious-but-valid" receiver) is authorized to trouble check queries adaptively. We show that adaptive SCF-PEKS may be generically built through anonymous identification-primarily based encryption first-class. That is, SCFPEKS can be constructed with none greater cryptographic primitive while as compared with the Abdulla et al. PEKS manufacturing (J. Cryptology 2008), despite the truth that adaptive SCF-PEKS calls for added functionalities. We moreover advocate distinctive adaptive SCFPEKS introduction, which isn't absolutely standard but is efficient compared with the number one. Finally, we instantiate an adaptive SCF-PEKS scheme (thru our 2d production) that achieves a similar degree of overall performance for the costs of the test way and encryption, compared with the (non-adaptive cozy) SCF-PEKS scheme via Fang et al. (CANS2009).

5) Off-line key-word guessing attacks on recent public key encryption with key-word seek schemes

AUTHORS: W.-C. Yau, S.-H. Heng, and B.-M. Goi,

The Public Key Encryption with Keyword Search Scheme (PEKS) changed into first proposed via Boneh et al. In 2004. This scheme solves the hassle of searching on statistics this is encrypted using a public key placing. Recently, Baek et al. Proposed a Secure Channel Free Public Key Encryption with Keyword Search (SCF-PEKS) scheme that eliminates the cozy channel for sending trapdoors. They later proposed each other stepped forward PEKS scheme that integrates with a public key encryption (PKE) scheme, known as PKE/PEKS. In this paper, we present off-line key-word

guessing assaults on SCF-PEKS and PKE/PEKS schemes. We show that outsider adversaries that capture the trapdoors despatched in a public channel can display encrypted key phrases with the resource of performing off-line key-phrase guessing attacks. While, insider adversaries can perform the assaults regardless the trapdoors sent in a public or cozy channel.

2.1 EXISTING SYSTEM:

- In a PEKS system, the usage of the receiver's public key, the sender attaches a few encrypted key terms (known as PEKS ciphertexts) with the encrypted records. The receiver then sends the trapdoor of a to-be-searched key-word to the server for facts looking. Given the trapdoor and the PEKS ciphertext, the server can test whether the key-word underlying the PEKS ciphertxt is same to the simplest decided on through the receiver. If so, the server sends the matching encrypted facts to the receiver.
- Baek et al. Proposed an EW PEKS scheme without requiring a cozy channel, it really is called a at ease channel-unfastened PEKS (SCF-PEKS).
- Rhee et al. Later more suitable Baek et al.'s safety version for SCF-PEKS wherein the attacker is authorized to reap the relationship between the non-venture cipher texts and the trapdoor.
- Byun et al.Added the off-line key-phrase guessing assault towards PEKS as key terms are chosen from a miles smaller area than passwords and customers usually use well-known keywords for looking files.

2.2. DISADVANTAGES OF EXISTING SYSTEM:

- Despite of being free from secret key distribution, PEKS schemes suffer from an inherent lack of confidence concerning the trapdoor key-phrase privateers, in particular interior Keyword Guessing Attack (KGA). The reason leading to the sort of protection vulnerability is that anyone who is aware of receiver's public key can generate the PEKS cipher text of arbitrary keyword himself.
- Specifically, given a trapdoor, the opposed server can choose out a guessing key-phrase from the keyword area after which use the keyword to generate a PEKS cipher text. The server then can check whether the guessing keyword is the one underlying the trapdoor. This guessing-then-sorting out device may be repeated till the high-quality key-word is observed.
- On one hand, despite the fact that the server can't exactly guess the key-word, it's

far nevertheless capable of understand which small set the underlying keyword belongs to and as a consequence the important thing-phrase privacy is not nicely preserved from the server. On the other hand, their scheme is impractical as the receiver has to regionally discover the matching cipher text through the usage of an appropriate trapdoor to clean out the non-matching ones from the set back from the server.

2.3 PROPOSED SYSTEM:

 The contributions of this paper are four-fold.

 We formalize a brand new PEKS framework named Dual-Server Public Key Encryption with Keyword Search (DS-PEKS) to cope with the safety vulnerability of PEKS.

 A new edition of Smooth Projective Hash Function (SPHF), referred to as linear and holomorphic SPHF, is brought for a frequent introduction of DS-PEKS.

 We show a acquainted manufacturing of DS-PEKS the use of the proposed Lin-Hom SPHF.

 To illustrate the feasibility of our new framework, and green instantiation of our SPHF based totally mostly on the Diffie-Hellman language is offered on this paper.

2.4 ADVANTAGES OF PROPOSED SYSTEM:

 All the triumphing schemes require the pairing computation all through the technology of PEKS cipher text and sorting out and for this reason are plenty much less green than our scheme, which does now not need any pairing computation.

 Our scheme is the most green in terms of PEKS computation. It is because of the truth that our scheme does now not encompass pairing computation. Particularly, the prevailing scheme calls for the most computation charge because of 2 pairing computation consistent with PEKS technology.

 In our scheme, regardless of the truth that we additionally require some different degree for the trying out, our computation rate is without a doubt lower than that of any gift scheme as we do not require any pairing computation and all of the searching paintings is dealt with via manner of the server.

3. MODULES:

- System Construction Module

- Semantic-Security in the direction of Chosen Keyword Attack
- Front Server
- Back Server

SYSTEM CONSTRUCTION MODULE

In the primary module, we extend the tool with the entities required to prove our gadget. 1) Cloud User: the client, who can be a character or a corporation at the start storing their facts in cloud and having access to the information. 2) Cloud Service Provider (CSP): the CSP, who manages cloud servers (CSs) and offers a paid garage area on its infrastructure to customers as a provider. We endorse a brand new framework, especially DS-PEKS, and present its formal definition and security fashions. We then define a modern-day variation of easy projective hash characteristic (SPHF). A time-honored production of DS-PEKS from LH-SPHF is tested with formal correctness evaluation and security proofs. Finally, we gift an inexperienced instantiation of DS-PEKS from SPHF.

SEMANTIC-SECURITY AGAINST CHOSEN KEYWORD ATTACK

In the module, we enlarge the semantic-security in competition to choose keyword attack which guarantees that no adversary is in a function to distinguish a key-word from every distinct one given the corresponding PEKS cipher text. That is, the PEKS cipher text does now not display any information about the underlying key-word to any adversary.

FRONT SERVER:

After receiving the query from the receiver, the front server pre-processes the trapdoor and all of the PEKS cipher texts the usage of its personal key, and then sends a few inner testing states to the decrease lower back server with the corresponding trapdoor and PEKS cipher texts hidden.

BACK SERVER:

In this module, the once more server can then determine which documents are queried thru the receiver the usage of its non-public key and the received internal locating out-states from the front server.

CONCLUSION

In 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 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.

FUTURE SCOPE 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. 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.

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, "Public key 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: Consistency properties, 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 on K-resilient IBE," in Proc. Int. Conf. Comput. Sci. Appl. (ICCSA), 2006, pp. 298–308.