Suneetha Thaduri* et al.
(IJITR) INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH
Volume No.4, Issue No.6, October – November 2016, 5201-5203.

A Well-Organized Preventive Scheme For KGA Using Hash Codes

SUNEETHA THADURI
Lecturer, Dept of CSE
Loyola Academy Degree and PG College
Secunderabad, T.S, India

HYMA BIRUDARAJU
Assistant Professor, Dept of MCA
Guru Nanak Institutions Technical Campus
Hyderabad, T.S, India

Abstract: **We introduce two games, namely semantic-security against selected keyword attack and indistinguishability against keyword guessing attack1 to capture the safety of PEKS ciphers text and trapdoor, correspondingly. Searchable file encryption is of growing interest for safeguarding the information privacy in secure searchable cloud storage. When it comes to trapdoor generation, as all of the existing schemes don't involve pairing computation, the computation price is reduced compared to PEKS generation. It's important to note the trapdoor generation within our plan is slightly greater than individuals of existing schemes because of the additional exponentiation computations. Within this paper, we investigate security of the well-known cryptographic primitive, namely, public key file encryption with keyword search (PEKS) that is very helpful in lots of applying cloud storage. Regrettably, it's been proven the traditional PEKS framework is affected with a natural insecurity known as inside keyword guessing attack (KGA) launched through the malicious server. To deal with this security vulnerability, we advise a brand new PEKS framework named dual-server PEKS (DS-PEKS). Then we show a normal construction of secure DS-PEKS from LH-SPHF. As one example of the practicality in our new framework, we offer a competent instantiation from the general framework from the Decision Diffie-Hellman-based LH-SPHF and show that it may attain the strong security against within the KGA. As the second primary contribution, we define a brand new variant from the smooth projective hash functions (SPHFs) known as straight line and homomorphic SPHF (LH-SPHF).**

Keywords: **Keyword Search; Secure Cloud Storage; Encryption; Inside Keyword Guessing Attack; Smooth Projective Hash Function; Diffie-Hellman Language;**

I. INTRODUCTION

Among the typical solutions may be the searchable file encryption which enables the consumer to retrieve the encrypted documents which contain the consumer-specified keywords, where because of the keyword trapdoor, the server will find the information needed through the user without understanding. Searchable file encryption could be recognized either in symmetric or uneven files encryption setting [1]. Precisely, users need to safely share secret keys which can be used for data file encryption. Otherwise they aren't able to share the encrypted data outsourced towards the cloud. To solve this issue, Boneh et al. introduced a far more flexible primitive, namely Public Key File encryption with Keyword Search (PEKS) that allows a person to look encrypted data within the uneven file encryption setting. Inside a PEKS system, while using receiver's public key, the sender attaches some encrypted keywords (known as PEKS cipher texts) using the encrypted data. The receiver then transmits the trapdoor of the to-be-looked keyword towards the server for data searching. Because of the trapdoor and also the PEKS cipher text, the server can test if the keyword underlying the PEKS ciphertxt is equivalent to the main one selected through the receiver. If that's the case, the server transmits the matching encrypted data towards the receiver. However, the truth is, finish users might not entirely trust the cloud storage servers and could choose to secure their data before uploading these to the cloud server to be able to safeguard the information privacy [2]. In spite of being free of secret key distribution, PEKS schemes are afflicted by a natural insecurity concerning the trapdoor keyword privacy, namely inside Keyword Guessing Attack (KGA). We formalize a brand new PEKS framework named Dual-Server Public Key File encryption with Keyword Search (DS-PEKS) to deal with the safety vulnerability of PEKS. We show a normal construction of DS-PEKS while using suggested Lin-Hom SPHF. A brand new variant of Smooth Projective Hash Function (SPHF), known as straight line and homomorphic SPHF, is introduced for any generic construction of DS-PEKS.

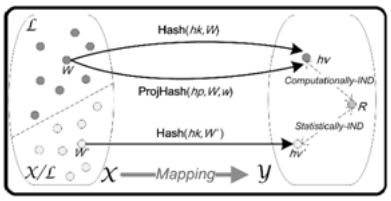

Fig.1.Proposed model

II. PROPOSED MODEL

A DS-PEKS plan mainly includes (Eigen, DS - PEKS, DS - Trapdoor, Front Test, and Backrest). To become more precise, the KeyGen formula generates the general publicOrpersonal key pairs of

the back and front servers rather of this from the receiver. Within the traditional PEKS, since there's just one server, when the trapdoor generation formula is public, then your server can launch a guessing attack against a keyword cipher text to recuperate the encrypted keyword. Another distinction between the standard PEKS and our suggested DS-PEKS would be that the test formula is split into two algorithms, Front Test and Back Test operated by two independent servers. This really is required for achieving security from the inside keyword guessing attack. Within the DS-PEKS system, upon getting a query in the receiver, the leading server pre-processes the trapdoor and all sorts of PEKS cipher texts having its private key, after which transmits some internal testing-states towards the back server using the corresponding trapdoor and PEKS cipher texts hidden. The rear server may then choose which documents are queried through the receiver having its private key and also the received internal testing-states in the front server [3]. You ought to observe that both front server and also the back server here should be "honest but curious" and won't collude with one another. More precisely, both servers carry out the testing strictly following a plan procedures but might be interested in the actual keyword. We ought to observe that the next security models also imply the safety guarantees from the outdoors adversaries that have less capacity when compared to servers. We introduce two games, namely semantic-security against selected keyword attack and indistinguishability against keyword guessing attack1 to capture the safety of PEKS ciphers text and trapdoor, correspondingly. Semantic-Security against Selected Keyword Attack. The PEKS cipher text doesn't reveal any details about the actual keyword to the foe. Indistinguishability against Keyword Guessing Attack. This security model captures the trapdoor reveals no details about the actual keyword towards the adversarial front server. Adversarial Back Server: The safety types of SS - CKA and IND - KGA when it comes to an adversarial back server act like individuals against an adversarial front server. Semantic-Security against Selected Keyword Attack. Here the SS - CKA experiment against an adversarial back server is equivalent to the main one against an adversarial front server with the exception that the foe is offered the non-public key from the back server rather of this from the front server. We omit the facts for simplicity. We make reference to the adversarial back server A within the SS - CKA experiment being an SS - CKA foe and define its advantage. Indistinguishability against Keyword Guessing Attack. Similarly, this security model aims to capture the trapdoor doesn't reveal any information towards the back server and therefore is equivalent to that from the front server with the exception that the foe owns the non-public key from the back server rather of this from the front server [4]. Therefore, we omit the facts here. Indistinguishability against Keyword Guessing Attack-II. Within our defined security perception of IND-KGA-II, it's needed that the malicious back server cannot learn any details about the actual two keywords active in the internal testing-condition. To begin with, we ought to observe that both keywords active in the internal-testing condition plays exactly the same role no matter their initial source Therefore, the job from the foe would be to guess the 2 underlying keywords within the internal testing condition in general, rather for each within the initial PEKS cipher text and also the initial trapdoor. Therefore, it's inadequate for that foe to submit couple of challenge keywords and therefore we must have the foe to submit three different keywords within the challenge stage and guess which two keywords are selected because of the challenge internal-testing condition. A main component of our construction for dual-server public key file encryption with keyword search is smooth projective hash function (SPHF), an idea created by Cramer and Shoup. Within this paper, we must have another essential property of smooth projective hash functions [5]. Precisely, we must have the SPHF to become pseudo-random. Within this paper, we introduce a brand new variant of smooth projective hash function. Additionally towards the original qualities, we consider two new qualities - straight line and homomorphic. Our plan is easily the most efficient when it comes to PEKS computation. For the reason that our plan doesn't include pairing computation. Particularly, the plan necessitates the most computation cost because of 2 pairing computation per PEKS generation. When it comes to trapdoor generation, as all of the existing schemes don't involve pairing computation, the computation price is reduced compared to PEKS generation. It's important to note the trapdoor generation within our plan is slightly greater than individuals of existing schemes because of the additional exponentiation computations. You ought to observe that this extra pairing computation is performed around the user side rather from the server. Therefore, it may be the computation burden for users who could use an easy device for searching data. Within our plan, although we require another stage for that testing, our computation price is really lower compared to any existing plan as we don't require any pairing computation and all sorts of searching jobs are handled through the server.

III. PREVIOUS STUDY

The very first PEKS plan without pairings was created by Di Crescenzo and Saraswat. The development comes from Cock's IBE plan which isn't very practical. The initial PEKS plan needs a

secure funnel to deliver the trapdoors. To beat this limitation, Baek et al. suggested a brand new PEKS plan without requiring a safe and secure funnel, which is called a safe and secure funnel-free PEKS (SCF-PEKS). The concept would be to add some server's public/private key pair right into a PEKS system. The keyword cipher text and trapdoor are generated while using server's public key and therefore just the server (designated tester) has the capacity to carry out the search. They enhanced the safety model by presenting the adaptively secure SCF-PEKS, in which a foe is permitted to issue test queries adaptively. Byun et al. introduced the off-line keyword guessing attack against PEKS as keywords are selected from the much smaller sized space than passwords and users usually use well-known keywords for searching documents [6]. The very first PEKS plan secure against outdoors keyword guessing attacks was suggested by Rhee et al. The idea of trapdoor indistinguishability was suggested and also the authors demonstrated that trapdoor in distinguish ability is really a sufficient condition for stopping outdoors keyword-guessing attacks. A possible option would be to propose a brand new framework of PEKS.

IV. CONCLUSION

A main component of our construction for dual-server public key file encryption with keyword search is smooth projective hash function (SPHF), an idea created by Cramer and Shoup. Within this paper, we must have another essential property of smooth projective hash functions. Within this paper, we suggested a brand new framework, named Dual-Server Public Key File encryption with Keyword Search (DS-PEKS), that may avoid the inside keyword guessing attack that is an natural vulnerability from the traditional PEKS framework. You ought to observe that this extra pairing computation is performed around the user side rather from the server. Therefore, it may be the computation burden for users who could use an easy device for searching data. We introduced a brand new Smooth Projective Hash Function (SPHF) and tried on the extender to create a normal DS-PEKS plan. A competent instantiation from the new SPHF in line with the Diffie-Hellman issue is also presented within the paper, which provides a competent DS-PEKS plan without pairings. When it comes to trapdoor generation, as all of the existing schemes don't involve pairing computation, the computation price is reduced compared to PEKS generation. It's important to note the trapdoor generation within our plan is slightly greater than individuals of existing schemes because of the additional exponentiation computations.

V. REFERENCES

[1] 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.

[2] 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.

[3] 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.

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

[5] 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.

[6] L. Fang, W. Susilo, C. Ge, and J. Wang, "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," Inf. Sci., vol. 238, pp. 221–241, Jul. 2013.

AUTHOR's PROFILE

Suneetha Thaduri is Working as Lecturer in Computer Science in Department of Computer Science, Loyola Academy Degree and P.G College. She has received her **M.Tech** in Computer Science and Engineering from Osmania University, University College of Engineering, Hyderabad, Telangana., India.

She has received her **M.C.A** in Computer Applications from Kakatiya University, University College of Engineering, Warangal, Telangana., India.

Her research areas include Cloud Computing, Grid Computing, Green Computing, Mobile Computing, Data Mining, Networking and Image Processing.

Hyma Birudaraju have done M.Tech, working as Asst.Prof in Guru Nanak Institutions Technical Campus. Her Area of Interests are Computer Networks, Data Mining.

