Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 10, October -2017

Achieving the strong security against data attacks in cloud Data Environments

L.LAVANYA LATHA[1] , R.SURESH[2]

[1](L.LAVANYA LATHA, DEPT OF COMPUTER SCIENCE AND ENGINEERING, CHADALAWADA RAMANAMA ENGINEERING COLLEGE,TIRUPATI, INDIA)

[2](R.SURESH, PROFESSOR, DEPT OF COMPUTER SCIENCE AND ENGINEERING, CHADALAWADA RAMANAMA ENGINEERING COLLEGE,TIRUPATI, INDIA)

Abstract: *Searchable encryption is of increasing interest for protecting the data privacy in secure searchable cloud storage. In this work, we investigate 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. Unfortunately, it has been shown that the traditional PEKS framework suffers from an inherent insecurity called inside Keyword Guessing Attack (KGA) launched by the malicious server. To address this security vulnerability, we propose a new PEKS framework named Dual-Server Public Key Encryption with Keyword Search (DS-PEKS). As another main contribution, we define a new variant of the Smooth Projective Hash Functions (SPHFs) referred to as linear and homomorphism SPHF (LH-SPHF). We then show a generic construction of secure DS-PEKS from LH-SPHF. To illustrate the feasibility of\ our new framework, we provide an efficient instantiation of the general framework from a DDH-based LH-SPHF and show that it can achieve the strong security against inside KGA.*

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

INTRODUCTION

In the existing system we present a data-centric access control solution with enriched role-based expressiveness in which security is focused on protecting user data regardless the Cloud service provider that holds it. Novel identity-based and proxy re-encryption techniques are used to protect the authorization model. Data is encrypted and authorization rules are cryptographically protected to preserve user data against the service provider access or misbehavior. The authorization model provides high expressiveness with role hierarchy and resource hierarchy support. The solution takes advantage of the logic formalism provided by Semantic Web technologies, which enables advanced rule management like semantic conflict detection. A proof of concept implementation has been developed and a working prototypical deployment of the proposal has been integrated within Google services. In the proposed system We formalize a new PEKS framework named Dual-Server Public Key Encryption with Keyword Search (DSPEKS)to address the security vulnerability of PEKS.A new variant of Smooth Projective Hash Function(SPHF), referred to as linear and homomorphism SPHF,is introduced for a generic construction of DS-PEKS. We show a generic construction of DS-PEKS usingthe proposed Lin-Hom SPHF.To illustrate the feasibility of our new framework,an efficient instantiation of our SPHF based on theDiffie-Hellman language is presented in this paper.

Definition of DS-PEKS

A DS-PEKS scheme mainly consists of (KeyGen, DS-PEKS, DS-Trapdoor; Front Test; Back Test). To be more precise, the KeyGen algorithm generates the public/private key pairs of the front and back servers instead of that of the receiver. Moreover, the trapdoor generation algorithm DS-Trapdoor defined here is public while in the traditional PEKS definition [5], [13], the algorithm Trapdoor takes as input the receiver's private key. Such a difference is due to the different structures used by the two systems. In the traditional PEKS, since there is only one server, if the trapdoor generation algorithm is public, then the server can launch a guessing attack against a keyword cipher text to recover the encrypted keyword. As a result, it is impossible to achieve the semantic security as defined in [5], [13]. However, as we will show later, under the DS-PEKS framework, we can still achieve semantic security when the trapdoor generation algorithm is public. Another difference between the traditional PEKS and our proposed DS-PEKS is that the test algorithm is divided into two algorithms, Front Test and Back Test run by two independent servers. This is essential for achieving security against the inside keyword guessing attack. In the DS-PEKS system, upon receiving a query from the receiver, the front server pre-processes the trapdoor and all the PEKS cipher texts using its private key, and then sends some internal testing-states to the back server with the

corresponding trapdoor and PEKS cipher texts hidden. The back server can then decide which documents are queried by the receiver using its private key and the received internal testing-states from the front server.

Definition 1 (DS-PEKS)

A DS-PEKS scheme is defined by the following algorithms.

Setup(1_). Takes as input the security parameter generates the system parameters P;

KeyGen(P): Takes as input the systems parameters P,outputs the public/secret key pairs (pkFS; skFS), and(pkBS; skBS) for the front server, and the back serverrespectively;

DS-PEKS(P; pkFS; pkBS; kw1): Takes as input P, the front server's public key pkFS, the back server's public key pkBS and the keyword kw1, outputs the PEKS ciphertext CTkw1 of kw1;

DS-Trapdoor(P; pkFS; pkBS; kw2): Takes as input P,the front server's public key pkFS, the back server's public key pkBS and the keyword kw2, outputs the trapdoor Tkw2 ;

FrontTest(P; skFS;CTkw1; Tkw2): Takes as input P,the front server's secret key skFS, the PEKS ciphertextn CTkw1 and the trapdoor Tkw2 , outputs the internal testing-state CITS;

BackTest(P;skBS;CITS): Takes as input P, the back server's secret key skBS and the internal testing-state CITS, outputs the testing result 0 or 1;

Correctness. It is required that for any keyword kw1; kw2, and CTkw1 DS-PEKS(P; pkFS; pkBS; kw1), Tkw2 DS-Trapdoor(P; pkFS; pkBS; kw2), we have

BackTest(P; skBS;CITS) =

(

1 kw1 = kw2;

0 kw1 6= kw2:

where CITS FrontTest(P; skFS;CTkw1 ; Tkw2):

Security Models

In this subsection, we formalize the following security models for a DS-PEKS scheme against the adversarial front and back servers, respectively. One should note that both the front server and the back server here are supposed to be "honest but curious" and will not collude with each other. More precisely, both the servers perform the testing strictly following the scheme procedures but may be curious about the underlying keyword. We should note that the following security models also imply the security guarantees against the outside adversaries which have less capability compared to the servers.

Adversarial Front Server:

In this part, we define the security against an adversarial front server. We introduce two games, namely semantic-security against chosen keyword attack and indistinguishability against keyword guessing attack1 to capture the security of PEKS cipher text and trapdoor, respectively.

Semantic-Security against Chosen Keyword Attack: In the following, we define the semantic-security against chosen keyword attack which guarantees that no adversary is able to distinguish a keyword from another one given the corresponding PEKS cipher text. That is, the PEKS cipher text does not reveal any information about the underlying keyword to any adversary.

Smooth Projective Hash Functions

A central element of our construction for dual-server public key encryption with keyword search is smooth projective hash function (SPHF), a notion introduced by Cramer and Shoup [23]. We start with the original definition of an SPHF.

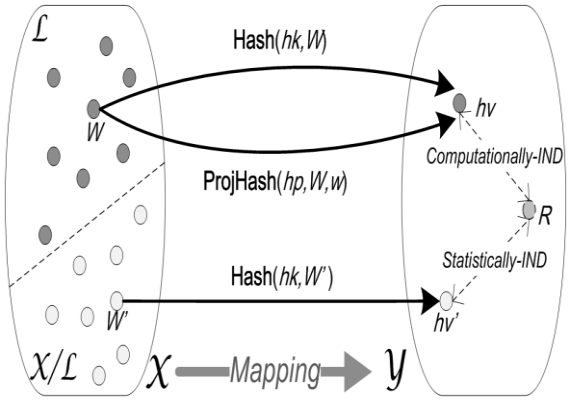

Fig. Smooth Projective Hash Function

As illustrated in Fig. 4, an SPHF is defined based on a domain $\mathcal{X}$ and an $\mathcal{NP}$ language $\mathcal{L}$, where $\mathcal{L}$ contains a subset of the elements of the domain $\mathcal{X}$, i.e., $\mathcal{L} \subset \mathcal{X}$. Formally, an SPHF system over a language $\mathcal{L} \subset \mathcal{X}$, onto a set $\mathcal{Y}$, is defined by the following five algorithms (SPHFSetup, HashKG, ProjKG, Hash, ProjHash):

- $\mathsf{SPHFSetup}(1^\lambda)$: generates the global parameters param and the description of an $\mathcal{NP}$ language instance $\mathcal{L}$;
- $\mathsf{HashKG}(\mathcal{L}, \mathsf{param})$: generates a hashing key hk for $\mathcal{L}$;
- $\mathsf{ProjKG}(\mathsf{hk}, (\mathcal{L}, \mathsf{param}))$: derives the projection key hp from the hashing key hk;
- $\mathsf{Hash}(\mathsf{hk}, (\mathcal{L}, \mathsf{param}), W)$: outputs the hash value $\mathsf{hv} \in \mathcal{Y}$ for the word W from the hashing key hk;
- $\mathsf{ProjHash}(\mathsf{hp}, (\mathcal{L}, \mathsf{param}), W, w)$: outputs the hash value $\mathsf{hv}' \in \mathcal{Y}$ for the word W from the projection key hp and the witness w for the fact that $W \in \mathcal{L}$.

The *correctness* of an SPHF requires that for a word $W \in \mathcal{L}$ with w the witness,

$$\mathsf{Hash}(\mathsf{hk}, (\mathcal{L}, \mathsf{param}), W) = \mathsf{ProjHash}(\mathsf{hp}, (\mathcal{L}, \mathsf{param}), W, w).$$

Another property of SPHFs is *smoothness*, which means that for any $W \in \mathcal{X} \backslash \mathcal{L}$, the following two distributions are statistically indistinguishable :

$$\mathcal{V}_1 = \{(\mathcal{L}, \mathsf{param}, W, \mathsf{hp}, \mathsf{hv}) | \mathsf{hv} = \mathsf{Hash}(\mathsf{hk}, (\mathcal{L}, \mathsf{param}), W)\},$$

$$\mathcal{V}_2 = \{(\mathcal{L}, \mathsf{param}, W, \mathsf{hp}, \mathsf{hv}) | \mathsf{hv} \xleftarrow{\$} \mathcal{Y}\},$$

CONCLUSION

In this paper, we proposed a new framework, named Dual- Server Public Key Encryption with Keyword Search (DSPEKS), 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 DSPEKSscheme. 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.

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 Information Security and Privacy - 20th Australasian Conference, ACISP, 2015, pp. 59–76.
[2] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in IEEE Symposium on Security and Privacy, 2000, pp. 44–55.

[3] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order-preserving encryption for numeric data," in Proceedings of the ACM SIGMOD International Conference on Management of Data, 2004, pp. 563–574.
[4] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," in Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, 2006, pp. 79–88.
[5] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in EUROCRYPT, 2004, pp. 506–522.
[6] R. Gennaro and Y. Lindell, "A framework for password-based authenticated key exchange," in 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 NDSS, 2004.
[8] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions," in CRYPTO, 2005, pp. 205–222.
[9] D. Khader, "Public key encryption with keyword search based on k-resilient IBE," in Computational Science and Its Applications - ICCSA, 2006, pp. 298–308.
[10] 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. Computers, vol. 62, no. 11, pp. 2266– 2277, 2013.
[11] G. D. Crescenzo and V. Saraswat, "Public key encryption with searchable keywords based on jacobi symbols," in INDOCRYPT, 2007, pp. 282–296.
[12] C. Cocks, "An identity based encryption scheme based on quadratic residues," in Cryptography and Coding, 2001, pp. 360–363.
[13] J. Baek, R. Safavi-Naini, and W. Susilo, "Public key encryption with keyword search revisited," in Computational Science and Its Applications - ICCSA, 2008, pp. 1249–1259.
[14] H. S. Rhee, J. H. Park,W. Susilo, and D. H. Lee, "Improved searchable public key encryption with designated tester," in ASIACCS, 2009, pp. 376–379.
[15] K. Emura, A. Miyaji, M. S. Rahman, and K. Omote, "Generic constructions of secure-channel free searchable encryption with adaptive security," Security and Communication Networks, vol. 8, no. 8, pp. 1547–1560, 2015.
[16] J. W. Byun, H. S. Rhee, H. Park, and D. H. Lee, "Off-line keyword guessing attacks on recent keyword search schemes over encrypted data," in Secure Data Management, Third VLDBWorkshop, SDM, 2006, pp. 75–83.
[17] W. Yau, S. Heng, and B. Goi, "Off-line keyword guessing attacks on recent public key encryption with keyword search schemes," in ATC, 2008, pp. 100–105.
[18] J. Baek, R. Safavi-Naini, andW. Susilo, "On the integration of public key data encryption and public key encryption with keyword search," in Information Security ISC, 2006, pp. 217–232.
[19] H. S. Rhee, W. Susilo, and H. Kim, "Secure searchable public key encryption scheme against keyword guessing attacks," IEICE Electronic Express, vol. 6, no. 5, pp. 237–243, 2009.
[20] H. S. Rhee, J. H. Park,W. Susilo, and D. H. Lee, "Trapdoor security in a searchable public-key encryption scheme with a designated tester," Journal of Systems and Software, vol. 83, no. 5, pp. 763–771, 2010.
[21] 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, 2013.
[22] I. R. Jeong, J. O. Kwon, D. Hong, and D. H. Lee, "Constructing PEKS schemes secure against keyword guessing attacks is possible?" Computer Communications, vol. 32, no. 2, pp. 394–396, 2009.
[23] R. Cramer and V. Shoup, "Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption," in EUROCRYPT, 2002, pp. 45–64.

