RESEARCH ARTICLE OPEN ACCESS

A Dual-Server Public-Key Encryption with Keyword Search for Secure Cloud Storage

[1]A.Senthil Kumar, [2]S.Vimal
[1]Asst.professor, Dept.of.Computer Science, Tamil University, Thanjavur-613010.
[2]Research Scholar, Dept.of.Computer Science, Tamil University, Thanjavur-613010.

Abstract:

Searchable encryption is of increasing interest for protecting the data privacy in secure searchable cloud storage. In this paper, 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 PEKS (DS-PEKS). As another main contribution, we define a new variant of the smooth projective hash functions (SPHFs) referred to as linear and homomorphic 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 Decision Diffie–Hellman-based LH-SPHF and show that it can achieve the strong security against inside the KGA.

Keywords— **Secure Cloud Storage; Encryption; Cloud Computing, Security.**

I. INTRODUCTION

Cloud storage outsourcing has turned into a well-known application for ventures and associations to lessen the weight of keeping up enormous information lately. Nonetheless, as a general rule, end clients may not so much trust the cloud capacity servers and may like to encode their information some time recently transferring them to the cloud server keeping in mind the end goal to ensure the information security. This as a rule makes the information usage more troublesome than the customary stockpiling where information is kept in the nonattendance of encryption. One of the regular arrangements is the searchable encryption which permits the client to recover the encoded reports that contain the client determined watchwords, where given the catchphrase trapdoor, the server can discover the information required by the client without decoding. Searchable encryption can be acknowledged in either symmetric then again deviated encryption setting. In watchword look on cipher text, known as Searchable Symmetric Encryption (SSE) and subsequently a few SSE plans were intended for enhancements. Despite the fact that SSE plans appreciate high proficiency, they experience the ill effects of muddled mystery key appropriation. Correctly, clients need to safely share mystery keys which are utilized for information encryption. Else they are not ready to share the scrambled information outsourced to the cloud. To determine this issue, presented a more adaptable primitive, to be specific Public Key Encryption with Keyword Search (PEKS) that empowers a client to seek encoded information in the awry encryption setting. In a PEKS framework, utilizing the collector's open key, the sender joins some encoded watchwords (allowed to as PEKS cipher texts) with the encoded information. The

beneficiary at that point sends the trapdoor of a to-be -sought catchphrase to the server for information seeking.

PROBLEM DEFINITION

This usually makes the data utilization more difficult than the traditional storage where data is kept in the absence of encryption. One of the typical solutions is the searchable encryption which allows the user to retrieve the encrypted documents that contain the user-specified keywords, where given the keyword trapdoor, the server can find the data required by the user without decryption. Searchable encryption can be realized in either symmetric or asymmetric encryption setting. In proposed keyword search on cipher text, known as Searchable Symmetric Encryption (SSE) and afterwards several SSE schemes were designed for improvements. Although SSE schemes enjoy high efficiency, they suffer from complicated secret key distribution. Precisely, users have to securely share secret keys which are used for data encryption. Otherwise they are not able to share the encrypted data outsourced to the cloud.

Disadvantages:

- SSE schemes enjoy high efficiency; they suffer from complicated secret key distribution.
- Users have to securely share secret keys which are used for data encryption. Otherwise they are not able to share the encrypted data outsourced to the cloud.

Public Key Encryption with Keyword Search (PEKS) that enables a user to search encrypted data in the asymmetric encryption setting. In a PEKS system, using the receiver's public key, the sender attaches some encrypted keywords (referred to as PEKS cipher texts) with the encrypted data. The receiver then sends the trapdoor of a to-be-searched keyword to the server for data searching. Given the trapdoor and the PEKS cipher text, the server can test whether the keyword underlying the PEKS cipher text is equal to the one selected by the receiver. If so, the server sends the matching encrypted data to the receiver.

Advantages

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

A new variant of Smooth Projective Hash Function (SPHF), referred to as linear and homomorphic SPHF, is introduced for a generic construction of DS-PEKS.

MODULES

We have 2 main modules in this project,

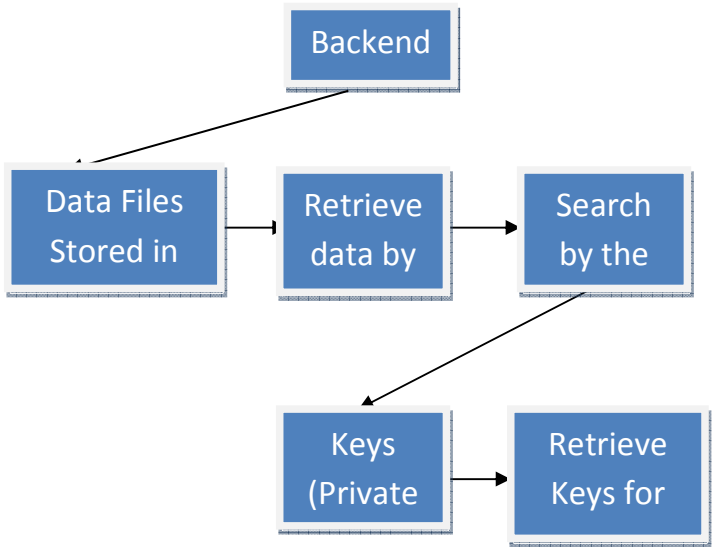
1. Ront Server Module
2. Ack Server Module

Module Description:

Front Server:

After receiving the query from the receiver, the front server pre-processes the trapdoor and all the PEKS ciphertexts using its private key, and then sends some internal testing-states to the back server with the corresponding trapdoor and PEKS ciphertexts hidden.

Backend Server:



Back Server:

In this module, 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.

V. CONCLUDION

To begin with, in the preparatory work where our nonspecific DS-PEKS development was exhibited, we indicated neither a solid development of the straight what's more, homomorphism SPHF nor a reasonable instantiation of the DS-PEKS structure. To fill this crevice and outline the plausibility of the system a direct and homomorphism dialect LDH can be gotten from the Diffie-Hellman supposition and at that point build a solid direct and homomorphism SPHF, alluded to as SPHFDH, from LDH. A formal verification that SPHFDH is right, smooth and pseudo-irregular development. We then present a solid DS-PEKS plot from SPHFDH. To investigate its execution, we first give a correlation between existing plans and our plan and after that assess its execution in trials. The preparatory adaptation to upgrade the presentation what's more, meaningfulness. In the related work part, analyzed to the preparatory rendition, include more written works and give a clearer characterization of the current plans in light of their security. An another structure, named Dual-Server Public Key Encryption with Keyword Search (DSPEKS) that can keep within catchphrase speculating assault which is an intrinsic helplessness of the conventional PEKS structure. We additionally presented another Smooth Projective Hash Function (SPHF) and utilized it to build a bland DSPEKS plot. An effective instantiation of the new SPHF in light of the Diffie-Hellman issue is additionally exhibited in the paper, which gives an effective DS-PEKS plot without pairings.

VI.REFERENCE

[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. 25th Annu. 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.

[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. Comput.*, vol. 62, no. 11, pp. 2266–2277, Nov. 2013.