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

Brijendra Singh Jadaun[1] Prof. Nitin Choudhary[2]
[1]Student [2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]Kopal Institute of Science & Technology, Bhopal (M.P), India

Abstract— Searchable encryption is one of fastly growing interest for protecting the data privacy in reliable searchable cloud storage. In this paper, we review the security of a well-known cryptographic primitive, namely, public key encryption with keyword search (PEKS) which is very helpful in many applications of cloud storage. Searchable encryption shown that the traditional PEKS framework suffers from an inherent insecurity called inside keyword guessing attack (KGA) launched by the malicious server. Searchable encryption is of elaborating eagerness for ensuring the information protection in secure searchable distributed storage. To refine this security vulnerability, we need to propose a new PEKS framework named dual-server PEKS (DS-PEKS).

Key words: Cloud Computing, Decryption, Encryption, Dual Server Encryption

I. INTRODUCTION

Cloud storage outsourcing has turned into a well-known application for scheme and associations to lessen the weight of keeping up vast information lately. Nonetheless, as a regular rule, end clients may not so much trust the cloud capacity servers and may like to encode their information some time recently transporting them to the cloud server keeping in mind the end goal to ensure the information security. For example, decoded client detail put away at the remote cloud server can be helpless against outer assaults started by unapproved outcasts and inside assaults started by the dishonest cloud service provider (CSPs) organizations. There are a few reports that proclaim information breaks identified with cloud servers, because of malignant assault, thieving or inward mistakes.

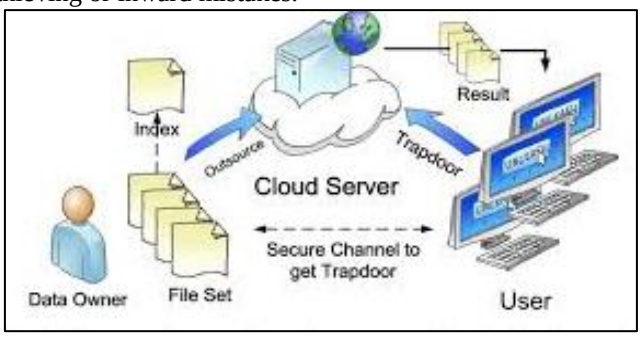

Fig. 1: Architecture of search over encrypted data in cloud computing

This raises consolation, information may contain extremely delicate individual association or data. In distributed cloud storage outsourcing has turned into a leading application for undertakings and associations to reducing the weight of keeping up enormous information lately. No withstanding, in all actuality, end clients may not by any means believe the cloud capacity servers and may want to crawling their information some time recently transferring them to the cloud server with a particular end goal to secure the information protection. This normally makes the information usage more troublesome than the conventional storage where information is kept in the nonappearance of encryption. One of the average arrangements is the searchable encryption which allows the client to recover the crawled records that contain the client shows the catchphrases, where given the watchword trapdoor, the server can discover the information need by the client without any problem. Below diagram show the encryption of data over a cloud computing.

II. LITERATURE SURVEY

S. Subashini n, V. KavithaCloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends Information Technology's (IT) existing capabilities. In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is.

Dawn Xiaodong Song David Wagner Adrian Perrig describe cryptographic schemes for the problem of searching on encrypted data and provide proofs of security for the resulting crypto systems. Our techniques have a number of crucial advantages. They are provably secure: they provide provable secrecy for encryption, in the sense that the untrusted server cannot learn anything about the plaintext when only given the ciphertext; they provide query isolation for searches, meaning that the untrusted server cannot learn anything more about the plaintext than the search result; they provide controlled searching, so that the untrusted server cannot search for an arbitrary word without the user's authorization; they also support hidden queries, so that the user may ask the untrusted server to search for a secret word without revealing the word to the server. The algorithms we present are simple, fast (for a document of length n, the encryption and search algorithms only need O(n) stream cipher and block cipher operations), and introduce almost no space and communication overhead, and hence are practical to use today.

Liming Fang a , Willy Susilo b,⇑ , Chunpeng Ge a , Jiandong Wang author make the following contributions. First, we define the strongest model of PEKS which is secure channel free and secure against chosen keyword attack, chosen ciphertext attack, and keyword guessing attack. In particular, we present two important security notions namely IND-SCF-CKCA and INDKGA. The former is to capture an inside adversary, while the latter is to capture an outside adversary. Intuitively, it should be clear that IND-SCF-

CKCA captures a more stringent attack compared to IND-KGA. Second, we present a secure channel free PEKS scheme secure without random oracle under the well-known assumptions, namely DLP, DBDH, SXDH and truncated q-ABDHE assumption. Our contributions fill the gap in the literature and hence, making the notion of PEKS very practical. We shall highlight that our scheme is IND-SCF-CKCA secure.

III. DESCRIPTION

Secret key distribution, PEKS schemes suffer from an inherent insecurity regarding the trapdoor keyword privacy, namely inside Keyword Guessing Attack (KGA). The reason leading to such security vulnerability is that anyone who knows receiver's public key can generate the PEKS cipher text of arbitrary keyword himself. Specifically, given a trapdoor, the adversarial server can choose a guessing keyword from the keyword space and then use the keyword to generate a PEKS cipher text. The Problem is to determine how to securely search any document from cloud in form of encrypted data with the help of dual servers. Dual Server-public key encryption with keyword search (PEKS).How to Store data in Secure form on cloud, How to Store data in Secure form on cloud.

IV. CONCLUSION

In this we review on Public-Key Encryption with Keyword Search for Secure Cloud Storage. The Existing manner on keyword-based encryption, which is widely used on the plaintext data, cannot be straightly applied on the encrypted data. Downloading all the data from the cloud and decrypt locally is clearly impractical, for future we can propose a new system that can prevent the inside keyword guessing attack which is an inherent vulnerability of the traditional PEKS framework

REFERENCES

[1] S. Subashini n, V. Kavitha" A survey on security issues in service delivery models of cloud computing"& 2010 Elsevier Ltd. All rights reserved
[2] Dawn Xiaodong Song David Wagner Adrian Perrig "Practical Techniques for Searches on Encrypted Data"0-7695-0665-8/00 $10.00 2000 IEEE.
[3] Liming Fang a , Willy Susilo b,⇑ , Chunpeng Ge a , Jiandong Wang "Public key encryption with keyword search secure against keyword guessing attacks without random oracle,"
[4] 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.
[5] 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.
[6] 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.
[7] 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
[8] 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.
[9] 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.
[10] 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

