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

Akash C. Deotale

Wainganga College Of Engineering And Management

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.

LITERATURE SURVEY

Cloud computing represents today's most exciting computing pattern shift in information technology[1]. but, security and privacy are perceived as primary obstacles to its large adoption[2]. Here, outline several critical security challenges and motivate further investigation of security solutions for a trustworthy public cloud environment[3]. cloud computing is the latest concept for the long-dreamed vision of computing as a usefulness. It is necessary to store information on information storage servers such as mail servers and record servers in encoded
frame to improve security and protection dangers. In any case, this typically suggests one needs to relinquish usefulness for security. For instance, if a customer wishes to recover just reports containing certain words, it was not beforehand known how to let the information stockpiling server play out the inquiry and answer the question without loss of information secrecy[4].
the issue of seeking on information that is encoded utilizing an public open key framework. Consider client Bob who sends email to client Alice scrambled under Alice's open key. An email passage needs to test whether the email contains the watchword \urgent" with the goal that it could course the email as needs be. Alice, then again does not wish to give the door the capacity to unscramble every one of her messages. We done and develop an instrument that empowers Alice to give a key to the portal that empowers the door to test whether the word \urgent"
is a watchword in the email without learning whatever else about the email. We allude to this system as Public Key Encryption with watchword Search. As another case, consider a mail server that stores different messages openly scrambled for Alice by others. Utilizing our instrument Alice can send the mail server a key that will empower the server to distinguish all messages containing some keyword which is we want to search[5]. The decent property in this plan permits the server to scan for a catchphrase, given the trapdoor. Thus, the verifier can just utilize an untrusted server, which makes this idea extremely down to earth. Taking after Boneh et
al's. work, there have been ensuing works that have been proposed to upgrade this idea. Two vital ideas incorporate the supposed catchphrase speculating assault and secure channel free, proposed by Byun et al. what's more, Baek et al., separately. The previous understands the way that by and by, the space of the catchphrases utilized is extremely constrained, while the last considers the evacuation of secure channel between the beneficiary and the server to
make PEKS down to earth. Lamentably, the current development of PEKS secure against catchphrase speculating

assault is just secure under the irregular prophet display, which does not mirror its security in this present reality. Moreover, there is no total definition that catches secure channel free PEKS plans that are secure against picked catchphrase assault, picked ciphertext assault, and against watchword speculating assaults, despite the fact that these thoughts appear to be the most pragmatic use of PEKS primitives[6]. A another system, called secure server-assignment open key encryption with catchphrase seek (SPEKS), was acquainted with enhance the security of dPEKS (which experiences the on-line catchphrase speculating assault) by characterizing another security demonstrate 'unique ciphertext indistinguishability'[7].

EXISTING SYSTEM:

- In a PEKS system, using the receiver's public key, the sender attaches some encrypted keywords (referred to as PEKS ciphertexts) 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 ciphertxt is equal to the one selected by the receiver. If so, the server sends the matching encrypted data to the receiver.
- Baek *et al.* proposed a ew PEKS scheme without requiring a secure channel, which is referred to as a secure channel-free PEKS (SCF-PEKS).
- Rhee *et al.* later enhanced Baek *et al*.'s security model for SCF-PEKS where the attacker is allowed to obtain the relationship between the non-challenge ciphertexts and the trapdoor.
- Byun *et al.*introduced the off-line keyword guessing attack against PEKS as keywords are chosen from a much smaller space than passwords and users usually use well-known keywords for searching documents.

DISADVANTAGES OF EXISTING SYSTEM:

- Despite of being free from 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 a security vulnerability is that anyone who knows receiver's public key can generate the PEKS ciphertext 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 ciphertext. The server then can test whether the guessing keyword is the one underlying the trapdoor. This *guessing-then-testing* procedure can be repeated until the correct keyword is found.
- On one hand, although the server cannot exactly guess the keyword, it is still able to know which small set the underlying keyword belongs to and thus the keyword privacy is not well preserved from the server. On the other hand, their scheme is impractical as the receiver has to locally find the matching ciphertext by using the exact trapdoor to filter out the non-matching ones from the set returned from the server.

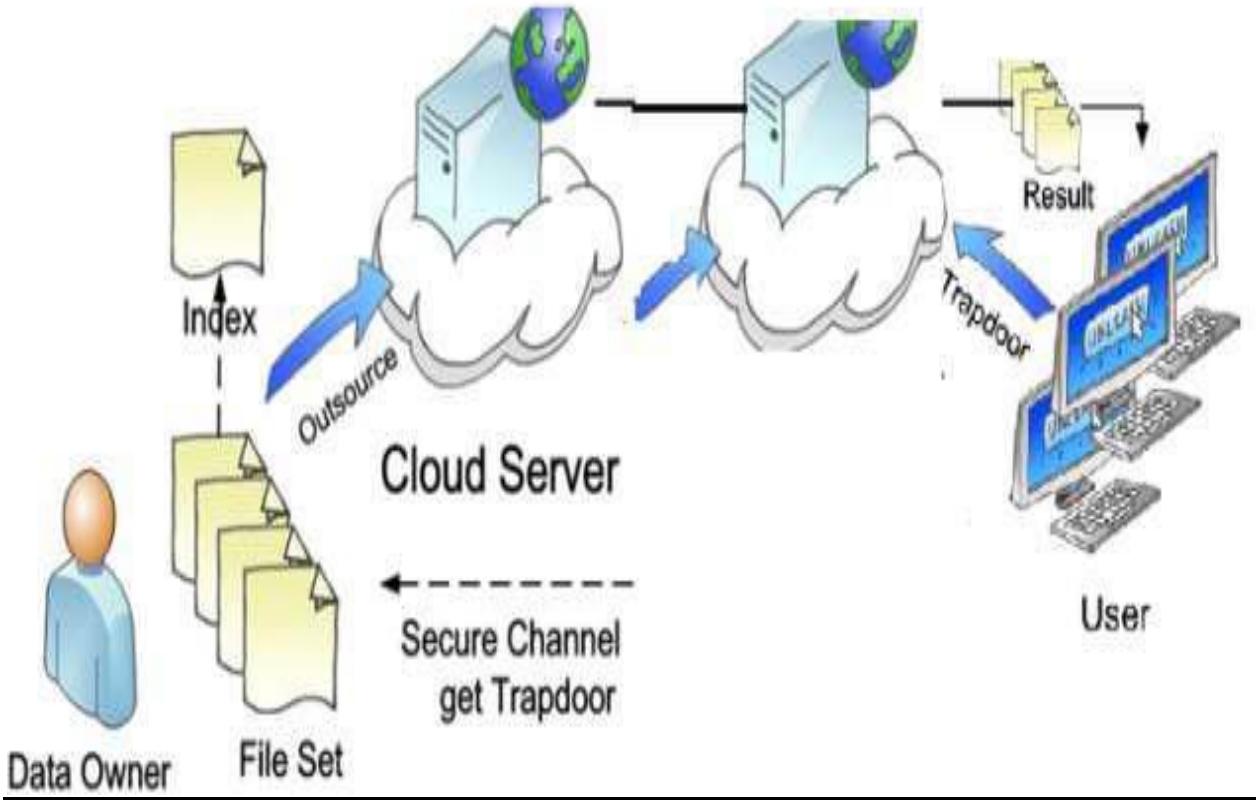
PROPOSED SYSTEM:

- The contributions of this paper are four-fold.
- 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.
- We show a generic construction of DS-PEKS using the proposed Lin-Hom SPHF.
- To illustrate the feasibility of our new framework, an efficient instantiation of our SPHF based on the Diffie-Hellman language is presented in this paper.

ADVANTAGES OF PROPOSED SYSTEM:

- All the existing schemes require the pairing computation during the generation of PEKS ciphertext and testing and hence are less efficient than our scheme, which does not need any pairing computation.
- Our scheme is the most efficient in terms of PEKS computation. It is because that our scheme does not include pairing computation. Particularly, the existing scheme requires the most computation cost due to 2 pairing computation per PEKS generation.
- In our scheme, although we also require another stage for the testing, our computation cost is actually lower than that of any existing scheme as we do not require any pairing computation and all the searching work is handled by the server.

SYSTEM ARCHITECTURE:



SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

- System : Pentium Dual Core.
- Hard Disk : 120 GB.
- Monitor : 15'' LED
- Input Devices : Keyboard, Mouse
- Ram : 1GB.

SOFTWARE REQUIREMENTS:

- Operating system : Windows 7.
- Coding Language : JAVA/J2EE

- Tool : Netbeans 7.2.1
- Database : MYSQL

REFERENCE:

1.Kamara S, Lauter K (2010) Cryptographic cloud storage. In: Sion R, Curtmola R, Dietrich S, Kiayias A, Miret,JM, Sako K, Sebé F (eds) Financial Cryptography and Data Security, LNCS 6054. Springer, Berlin, Heidelberg, pp 136–149.

2. Hacigümüș H, Iyer B, Li C, Mehrotra S (2002) Executing sql over encrypted data in the database-serviceprovider model. In: Proceedings of SIGMOD, ACM, pp 216–227.

3. Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl 34:1–11.

4. 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. *Vol-3 Issue-1 2017 IJARIIE-ISSN(O)-2395-4396* 3667 www.ijariie.com 355

5. D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in EUROCRYPT, 2004, pp. 506–522.

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, 2013.

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–

8.Rongmao Chen, Yi Mu, *Senior Member, IEEE*, Guomin Yang, *Member, IEEE*, Fuchun Guo, and Xiaofen Wang, "Dual-Server Public-Key Encryption With Keyword Search for Secure Cloud Storage", **IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 4, APRIL 2016.**

9. ISSN(Online) : 2319-8753 ISSN (Print) : 2347-6710 International Journal of Innovative Research in Science, Engineering and Technology*(An ISO 3297: 2007 Certified Organization)*
Vol. 6, Special Issue 12, July 2017 Copyright to IJIRSET www.ijirset.com 1 Two Independent Server Public Key Encryption and Keyword Search for Secure Cloud Access Swetha N1, Prof. Sreelatha P K 2 P G Student, Dept. of CSE, SVIT College, Rajanukunte, Bengaluru, India1
Asst. Prof, Dept. of CSE, SVIT College, Rajanukunte, Bengaluru, India 2

10. *ISSN (e): 2250 – 3005 || Volume, 07 || Issue, 08|| August – 2017 || International Journal of Computational Engineering Research (IJCER)* www.ijceronline.com Open Access Journal Page 40 Secure Keyword Search with Public Key Encryption by Cloud storage *T. Nagamani1, Dr. V.Senthilkumar2, S.Varuna3 *1Assistant Professor, Department of Computer Science and Engineering 2Assistant Professor (Sr.G), Department of Civil Engineering 3Assistant Professor, Department of Computer Science and Engineering Bannari Amman Institute of Technology, Sathyamangalam, Erode, India Corresponding Author: *T. Nagaman.*

11. International Journal of Computational Intelligence Research ISSN 0973-1873 Volume 13, Number 5 (2017), pp. 1271-1282 © Research India Publications http://www.ripublication.com
Secure Keyword Search Using Dual Encryption in Cloud: An Approach Husna Tariq
Department of Computer Science, Jamia Hamdard, Hamdard Nagar, New Delhi, 110062, India
Dr. Parul Agarwal* *Department of Computer Science, Jamia Hamdard, Hamdard Nagar, New Delhi, 110062, India *Corresponding Author*