© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 06 | April - June 2017
Paper is available at www.jrps.in | Email : info@jrps.in

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

Brijendra Singh Jadaun
Kopal Institute of Science & Technology
CSE,Bhopal (M.P)

Prof. Nitin Choudhary
Kopal Institute of Science & Technology
CSE,Bhopal (M.P)

Abstract: Searchable encryption is of expanding passion for ensuring the information security in secure searchable distributed 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. 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 homomorphism SPHF (LH-SPHF).We then show a general construction of secure DS-PEKS from LH-SPHF. To explain the viability 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 attain the strong security against inside the KGA.

Keywords: Cloud Computing, Keyword Guessing Attack, SPHFs, DS-PEKS

ISSN : 2278-6848 03
9 772278 684800
© International Journal for Research Publication and Seminar

1. INTRODUCTION

To make data management scalable in cloud computing, reduplication has been a well-known technique and has attracted more and more attention recently. Data reduplication is a specialized data compression technique for eliminating duplicate copies of repeating data in storage. The technique is used to improve storage utilization and can also be applied to network data transfers to reduce the number of bytes that must be sent. Instead of keeping multiple data copies with the same content, reduplication eliminates redundant Cloud computing provides seemingly unlimited “virtualized” resources to users as services across the whole Internet, while hiding platform and implementation details. Today’s cloud service providers offer both highly available storage and massively parallel computing resources at relatively low costs. As cloud

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 06 | April - June 2017
Paper is available at www.jrps.in | Email : info@jrps.in

computing becomes prevalent, an increasing amount of data is being stored in the cloud and shared by users with specified.

The user is able to find a duplicate for this file if and only if there is a copy of this file and a matched privilege stored in cloud. For example, in a company, many different privileges will be assigned to employees. In order to save cost and efficiently management, the data will be moved to the storage server provider (SCSP) in the public cloud with specified privileges and the reduplication technique will be applied to store only one copy of the same file. Because of privacy consideration, some files will be encrypted and allowed the duplicate check by employees with specified privileges to realize the access control. Traditional reduplication systems based on convergent encryption, although providing confidentiality to some extent, do not support the duplicate check with differential privileges. In other words, no differential privileges have been considered in the reduplication based on convergent encryption technique. It seems to be contradicted if we want to realize both reduplication and differential authorization Duplicate check at the same time.

2. PROBLEM DEFINITION

The problem of reduplication with differential privileges in cloud computing, we consider a hybrid cloud architecture consisting of a public cloud and a private cloud. Unlike existing data reduplication systems, the private cloud is involved as a proxy to allow data owner/users to securely perform duplicate check with differential privileges. Such architecture is practical and has attracted much attention from researchers. The data owners only outsource their data storage by utilizing public cloud while the data operation is managed in private cloud. A new reduplication system supporting differential duplicate check is proposed under this hybrid cloud architecture where the S-CSP resides in the public cloud. The user is only allowed to perform the duplicate check for files marked with the corresponding privileges

3. PROPOSED WORK

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

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 06 | April - June 2017
Paper is available at www.jrps.in | Email : info@jrps.in

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.

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 homomorphism SPHF, is introduced for a generic construction of DS-PEKS.Below fig1.show the DFD of Proposed work and fig2 show Implementation of Proposed work.

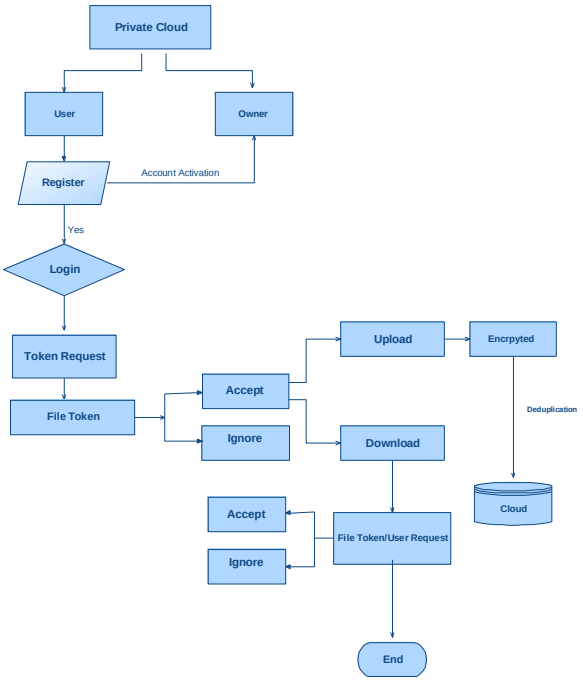

Fig1: DFD of Proposed work

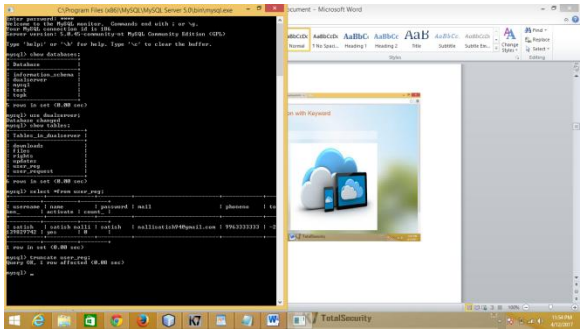

Fig 2: Implemntation of Proposed work

4. CONCLUSION & FUTURE WORK

In this paper, the notion of authorized data reduplication was proposed to protect the data security by including differential privileges of users in the duplicate check. We also presented several new reduplication constructions supporting authorized duplicate check in hybrid cloud architecture, in which the duplicate-check tokens of files are generated by the private cloud server with private keys. Security analysis demonstrates that our schemes are secure in terms of insider and outsider attacks specified in the proposed security model. As a proof of concept, we implemented a prototype of our proposed authorized duplicate check scheme and conduct tested experiments on our prototype. We showed

that our authorized duplicate check scheme incurs minimal overhead compared to convergent encryption and network transfer.

5. 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.

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. 59–76.

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. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, “Orderpreserving encryption for numeric data,” in Proceedings of the ACM SIGMOD International Conference on Management of Data, 2004, pp. 563–574.

7.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.

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

9. 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.

10. R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang, “A new general framework for secure public key encryption with keyword

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 08 Issue: 06 | April - June 2017
Paper is available at www.jrps.in | Email : info@jrps.in

search," in Information Security and Privacy - 20th Australasian Conference, ACISP, 2015, pp. 59– 76.

11. G. D. Crescenzo and V. Saraswat, "Public key encryption with searchable keywords based on jacobi symbols," in INDOCRYPT, 2007, pp. 282–296