© 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

1. INTRODUCTION

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

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