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

PABBU SREENU¹, K. S. SADA SHIVA RAO², D. PRATIBHA³

¹PG Scholar, Dept of CSE, Sri Indu Institute of Engineering & Technology, Hyderabad, TS, India, Email: pabbusrinu376@gmail.com.
²Professor, Dept of CSE, Sri Indu Institute of Engineering & Technology, Hyderabad, TS, India, Email: hodcsiiet@gmail.com.
³Associate Professor, Dept of CSE, Sri Indu Institute of Engineering & Technology, Hyderabad, TS, India, Email: send2prathibha@gmail.com.

Abstract: Now a day’s there will be growing popularity of cloud computing, large number of users and data owners are motivated to outsource their data to cloud servers for large convenience and reduced cost required for data management. However, important data should be encrypted before outsourcing for privacy requirements, which uses data utilization technique like keyword-based document retrieval. Searchable encryption is of expanding enthusiasm for ensuring the information protection in secure searchable distributed storage. In this work, we explore the security of an outstanding cryptographic primitive, in particular Public Key Encryption with Keyword Search (PEKS) which is exceptionally helpful in numerous utilizations of distributed storage. Astonishingly, it has been demonstrated that the customary PEKS system experiences an indisputable instability called inside Keyword Guessing Attack (KGA) propelled by the malevolent server. To address this security vulnerability, we propose another PEKS structure named Dual-Server Public Key Encryption with Keyword Search (DS-PEKS). As another fundamental commitment, we characterize another variation of the Smooth Projective Hash Functions (SPHFs) referred to as straight and homomorphism SPHF (LH-SPHF). We then demonstrate a bland development of secure DS-PEKS from LH-SPHF. To represent the possibility of our new structure, we give a proficient instantiation of the general system from a DDH-based LH-SPHF and demonstrate that it can accomplish the solid security against inside KGA.

Keywords: Keyword Search, Secure Cloud Storage, Encryption, Inside Keyword Guessing Attack, Smooth Projectivehash Function, Diffie-Hellman Language.

I. INTRODUCTION

With the fast improvement of distributed computing and portable systems administration innovations, clients tend to get to their put away information from the remote distributed storage with cell phones. The fundamental favorable position of distributed storage is its pervasive client availability furthermore it’s for all intents and purposes boundless information stockpiling capacities. Notwithstanding such advantages gave by the cloud, the real test that remaining parts is the worry over the secrecy and protection of information while embracing the distributed storage administrations. For example, decoded client information put away at the remote cloud server can be defenseless 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 affirm information breaks identified with cloud servers, because of malignant assault, burglary or inward mistakes. This raises sympathy information may contain extremely delicate individual association/data. Distributed cloud storage outsourcing has turned into a prominent application for undertakings and associations to lessen 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 scramble their information some time recently transferring them to the cloud server with a specific 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 permits the client to recover the scrambled records that contain the client indicated catchphrases, where given the watchword trapdoor, the server can discover the information required by the client without any problem.

II. LITERATURE SURVEY

Cloud computing represents today’s most exciting computing pattern shift in information technology. But, security and privacy are perceived as primary obstacles to its large adoption. Here, outline several critical security challenges and motivate further investigation of security solutions for a trustworthy public cloud environment 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

Copyright © 2017 IJIT. All rights reserved.
server play out the inquiry and answers the question without
loss of information secrecy. The issue of seeking on
information that is encoded utilizing a 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.

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
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 etal., 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 cipher text assault,
and against watchword speculating assaults, despite the fact
that these thoughts appear to be the most pragmatic use of
PEKS primitives. 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
cipher text in distinguish ability'.

III. EXISTING AND PROPOSED SYSTEMS
A. Existing System
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.

B. Proposed System
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.

- 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 holomorphic SPHF, is
  introduced for a generic construction of DS-PEKS.

C. Modules
We have 2 main modules in this project.
1. Front Server Module
2. Back Server Module

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

IV. RESULT

Fig 1.
Keyword Search for Secure Cloud Storage with Dual-Server Public Key Encryption

Fig 2.

Fig 3.

Fig 4.

Fig 5.

Fig 6.

Fig 7.
Keyword Search for Secure Cloud Storage with Dual-Server Public Key Encryption

Fig 26.

Fig 27.

Fig 28.

Fig 29.

Fig 30.

Fig 31.
V. CONCLUSION

In this paper, we proposed another structure, named Dual-Server Public Key Encryption with Keyword Search (DSPEKS) that can keep within catchphrase speculation 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. REFERENCES

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