A Survey on Dual-Server Public-Key Encryption with Keyword Search for Secure Cloud Storage and Privacy-Preserving Healthcare Data Management

Dr. Rafael Mendes[1]*
Dr. Hana Kim[1]
[1] University of Singapore, Department of Cybersecurity and Cloud Computing for Biomedical Data Systems, Singapore, Singapore

ABSTRACT

Searchable encryption is of accelerating interest for shielding the information privacy in secure searchable cloud storage. In this paper, we have a tendency to investigate the safety of a widely known scientific discipline primitive, namely, public key encryption with keyword search (PEKS) that is extremely helpful in several applications of cloud storage. Unfortunately, it's been shown that the standard PEKS framework suffers from AN inherent insecurity referred to as within keyword guesswork attack (KGA) launched by the malicious server. To address this security vulnerability, we have a tendency to propose a brand new PEKS framework named dual-server PEKS (DS-PEKS). As another main contribution, we have a tendency to outline brand new variant of the sleek projective hash functions (SPHFs) named as linear and homomorphic SPHF (LH-SPHF). We then show a generic construction of secure DS-PEKS from LH-SPHF. To illustrate the practicability of our new framework, we offer an economical mental representation of the overall framework from a choice Diffie–Hellman-based LH-SPHF and show that it can do the strong security against inside the KGA.

I. INTRODUCTION

Cloud storage utilizing has become a popular application for enterprises and organizations to reduce the burden of maintaining big data in recent years.

However, in reality, end users may not entirely trust the cloud storage servers and should like better to cypher their information before uploading them to the cloud server so as to guard the data privacy.

This usually makes the data utilization more difficult than the standard storage wherever information is unbroken in the absence of encryption.

One of the typical solutions is the searchable encoding that permits the user to retrieve the encrypted documents that contain the user-specified keywords, where given the keyword trapdoor, the server cannotice the info needed by the user while not decoding.

Searchable encoding is accomplished in either symmetrical or uneven encoding setting. In projected keyword search on ciphertext, known as Searchable Symmetric Encryption (SSE) and afterwards several SSE schemes were designed for improvements.

Although south southeast schemes relish high potency, they suffer from sophisticated secret key distribution. Precisely, users have to securely share personal keys which are used for data encryption.

Otherwise they're not capable to share the encrypted information outsourced to the cloud. To resolve this problem, Bonehetal introduced a more flexible primitive, namely Public Key encoding with Keyword Search (PEKS) that allows 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 ciphertexts) with the encrypted data. The receiver then passes the trapdoor of a to-be-searched keyword to the server for data searching.

Given the trapdoor and the PEKS ciphertext, the server will check whether or not the keyword underlying the PEKS ciphertext is equal to the one selected by the receiver. If so, the server gives the matching encrypted data to the receiver.

II. LITERATURE SURVEY

Cloud computing represents today's most enjoyable computing pattern shift in info technology. But, security and privacy area unit perceived as primary obstacles to its giant adoption. Here, define many essential security challenges and encourage additional investigation of security solutions for a trustworthy public cloud setting. cloud computing is that the latest thought for the long-dreamed vision of computing as a quality.

It is necessary to store info on info storage servers like mail servers and record servers in encoded frame to boost security and protection dangers.The issue of seeking on info that's encoded utilizing associate degree public open key framework. Consider shopper Bob WHO sends email to shopper Alice disorganised beneath Alice's open key. An email passage has to take a look at whether or not the e-mail contains the watchword urgent" with the goal that it might course the e-mail as wants be. Alice, except doesn't want to present the door the capability to unscramble all of her messages.

We done associate degreed develop an instrument that empowers Alice to present a key to the portal that empowers the door to check whether or not the word urgent" could be a watchword in the e-mail while not learning no matter else concerning the email. We hint to the present system as Public Key cryptography with watchword Search.

As another case, contemplate a mail server that stores completely different messages brazenly disorganised for Alice by others.

Utilizing our instrument Alice will send the mail server a key which will empower the server to differentiate all messages containing some keyword that is we wish to go looking.

The good property during this set up permits the server to scan for a phrase, given the trapdoor. Thus, the admirer will simply utilize associate degree untrusted server, that makes this idea very all the way down to earth.

Taking after Boneh et al's. work, there are succeeding works that are planned to upgrade this idea. Two vital ideas incorporate the supposed catchphrase speculating assault and secure channel free, proposed by Byunetal. what's more, Baek et al., separately.

The previous understands the means that by and by, the area of the catchphrases utilised is very forced, whereas the last considers the evacuation of secure channel between the beneficiary and also the server to create PEKS all the way down to earth.

Lamentably, the present development of PEKS secure against phrase speculating assault is simply secure beneath the irregular prophet show, which does not mirror its security in this present reality. Moreover, there's no total definition that catches secure channel free PEKS plans that area unit secure against picked phrase 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.

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'.

III. EXISTING SYSTEM

In a PEKS system, victimization the receiver's public key, the sender attaches some encrypted keywords (referred to as PEKS ciphertexts) with the encrypted information.

The receiver then sends the trapdoor of a to-be-searched keyword to the server for information looking out.

Given the trapdoor and therefore the PEKS ciphertext, the server will check whether or not the keyword underlying the PEKS ciphertxt is adequate to the one elect by the receiver. If so, the server sends the matching encrypted information to the receiver.

Baek et al. proposed a brand new PEKS theme while not requiring a secure channel, that is cited as a secure channel-free PEKS (SCF-PEKS).

IV. PROPOSED SYSTEM

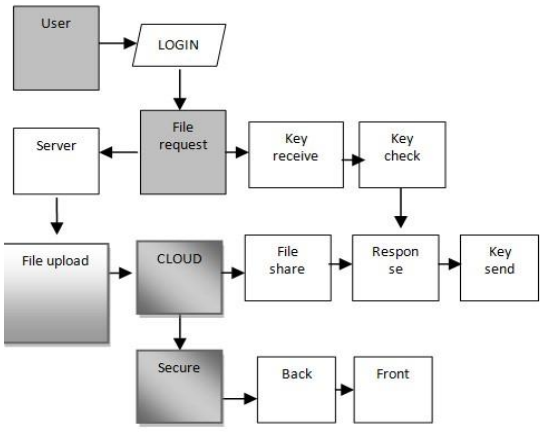
The contributions of this paper are four-fold.

- We formalize a new PEKS framework named DualServer Public Key Encryption with Keyword Search (DS-PEKS) to address the security vulnerability of PEKS.
- A new variant of sleek Projective Hash perform(SPHF), observed 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 DiffieHellman language is presented in this paper.

V. RELATED WORK

Cloud computing is that the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet).

The name comes from the common use of a cloud-shaped image as Associate in Nursing abstraction for the complicated infrastructure it contains in system diagrams.



VI. ALGORITHM

A DS-PEKS theme is outlined by the subsequent algorithms.

- Setup(1_). Takes as input the safety parameter nine, generates the system parameters P.
- KeyGen(P): Taking a input the systems parameters P,outputs the public/secret key pairs (pkFS; skFS), and (pkBS; skBS) for the front server, and also the back server respectively;
- DS-PEKS(P; pkFS; pkBS; kw1): Takes as input P, the front server's public key pkFS, the rear server's public keypkBS and also the keyword kw1, outputs the PEKS ciphertextCTkw1 of kw1;
- DS-Trapdoor(P; pkFS; pkBS; kw2): Takes as input P, the front server's public key pkFS, the rear server's public key pkBS and also the keyword kw2, outputs the trapdoorTkw2 ;
- FrontTest(P; skFS;CTkw1 ; Tkw2): Taking a input P, the front server's secret key skFS, the PEKS ciphertextCTkw1 and also the trapdoor Tkw2 , outputs the inner testing-state CITS;

- BackTest(P; skBS;CITS): Takes as input P, the rear server's secret key skBS and also the internal testing-state CITS, outputs the testing result zero or 1.

VII. MODULES

- HOME.
- DATA OWNER MODULE.
- DATA USER MODULE.
- CLOUD STORAGE

Data owner module:

a) Registration Module:

Registration module is used foradmin authentication purpose in which administrator can only access this admin module.

It contains authentication type and personal details of admin such as name, designation, mail id, phone number, address, username, password, date of birth, photo and also it can be stored and maintained in database.

The person who is authenticating it will access it by using username and password.

b) Login Module:

This module checks the admin register page by checking with mail id and password which is already stored in database.

It true data is authenticated that allows to go for main admin module or otherwise that will stay in current page by showing up alert message as Invalid User.

c) Home Module:

In this module Data Owner Home this contains Basic functionalities of cloud that can be helpful for data Owner who is logged on already in session.

d) Upload Module:

In which,the files are uploaded in format of file name,keywords.In this case single keyword does not helps in the searching to avoid this we are using three types of keyword to fetch the file.The file are stored in the encrypted formats.

e) My Files Module:

My Files page shows files which is uploaded by particular data user.

f) Approvals Module:

In this module, the request send by the data user can be authenticated by the data owner. Either accepts the request or rejects the request.

g) Logout:

This module which completely moves you out from the data owner session to the home session.

Data user module:

a) Registration Module:

Registration module is used for data user authentication purpose in which administrator can only access this admin module.

It contains authentication type and personal details of admin such as name, designation, mail id, phone number, address, username, password, date of birth, photo and also it can be stored and maintained in database.

The person who is authenticating it will access it by using username and password.

b) Login Module:

This module checks the admin register page by checking with mail id and password which is already stored in database.

It true data is authenticated that allows to go for main admin module or otherwise that will stay in current page by showing up alert message as Invalid User.

c) Home Module:
In this module Data user Home this contains Basic functionalities of cloud that can be helpful for data Owner who is logged on already in session.

d) Search:
Search module, in which you can search the file that you want. The search request is send as query that finds the data from the cloud.
Shows your approximate search, you can send request to the file so that particular data owner either accept/decline request as their wish.

e) Requested files:
This shows your file is either accepted or not.If accepted you can view file by particular generated decryption key so that encrypted file will be downloaded as decrypted the readable format.

g) Logout:
This module which completely moves you out from the data user session to the home session.

Cloud storage module:
This module completely shows the accurate data stored in the cloud storage..This help you search file that you needed.

These are divided into two different servers such as server1 and server2.
*** Server 1**
The Server1 only maintenance the database of the owner and user details, file details and also Encryption/decryption key details.

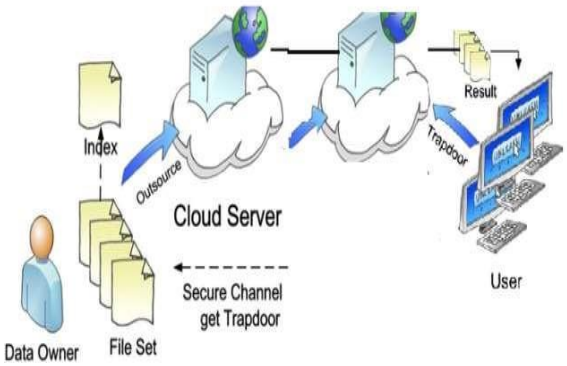
*** Server 2**
The Server2 only maintenance the file storage space of an encrypted data.

VIII. TOOLS AND TECHNOLOGY USED

In this project I used:
Java Technology:

- Java technology is each the artificial language and a platform.
- The Java programming language may be a problem-oriented language
- SQL Management Server 2014 technologies

IX. SYSTEM ARCHITECTURE



Data Owner:
Register with cloud server and login(username should be unique). Send request to Public key generator (PKG) to come up with Key on the user name.
Browse file and request Public key to write the info, transfer information to cloud service supplier. Verify the data from the cloud .

Public Key Generator:
Receive request from the users to come up with the key,Store all keys supported the user names. Check the username and provide the private key.
Revoke the tip user (File Receiver if they struggle to hack enter the cloud server and international organization revoke the user when change the non-public key for the corresponding file based on the user).

Key Update:
Receive all files from the info owner and store all files. Check the info integrity within the cloud and inform to finish user regarding the info integrity.
Send request to PKG to Update the non-public key of the user supported the date parameter (Give some date to update non-public Key).
List all files, List all updated non-public Key details supported the date and users, List all File attackers and File Receive Attackers.

X. CONCLUSION

In this paper, we have a tendency to projected a replacement framework, named Dual-Server Public Key cryptography with Keyword Search (DS-PEKS), which will forestall the within keyword estimate attack that is associate inherent vulnerability of the normal PEKS framework. We also introduced a new Smooth Projective Hash Function (SPHF) and used it to construct a generic DSPEKS scheme.

An efficient instantiation of the new SPHF based on the Diffie-Hellman problem is also presented in the paper, which gives an efficient DSPEKS scheme without pairings.

XI. FUTURE ENHANCEMENT

The future scope which are developed in future are listed below.

- By using this DS-PEKS method, we protect and secured the data used and stored in the cloud.
- It will prevent from the hacking the data which are stored in cloud and it is used safely.
- It stores the data and separated into the dual server which are encrypted

REFERENCES

1. *K. Emura, A. Miyaji, M. S. Rahman, and K. Omote, "Generic developed of prevent channel free searchablecryptography with modifying security," Secure. Commune. Network 1547–1560, 2015.*
2. *Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. J NetwComputAppl 34:1–11.*
3. *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.*
4. *W. Yau, S. Heng, and B. Goi, "Off-line keyword guessing attacks on recent public key encryption with keyword search schemes," in ATC, 2008.*
5. *J.Baek, R.Safavi- Naini, and W.Susilo," On the integration of public key data encryption and public key encryption with keyword search," in Information Security ISC, 2006, pp. 217–232.*
6. *H.S.Rhee, J.H.Park, W.Susilo, and D.H.Lee, "Trap door security in a searchable public-key encryption strategy with a styled tester," Journal of Systems and S/W, vol. 83, no. 5, pp. 763–771, 2010. [21]*
7. *L.Fang, W.Susilo, C.Ge, and J.Wang, "Public key encrpytion with keyword search secure against keyword assumption attacks without random oracle," Inf. Sci., vol. 238, pp. 221–241, 2013.*