Privacy Preserving Encrypted Keyword Search Schemes

Dipti D. Mehare[1], Prof. A. V. Deorankar[2]

[1]P.G. Scholar, Department of Computer Science, Government college of Engineering, Amravati, Maharashtra, India
[2]Assistant Professor, Department of Information Technology, Government college of Engineering, Amravati Maharashtra, India

---***---

Abstract - *Search over encrypted data is a technique of great interest in the cloud computing era, because many believe that sensitive data has to be encrypted before outsourcing to the cloud servers in order to ensure user data privacy. A secure and privacy preserving encrypted keyword search scheme suitable for cloud storage. In this secure and efficient privacy preserving search keyword on encrypted data approach contains three participants are there: 1) user 2) key server 3) CSP. A cloud service provider (CSP), whose purpose is mainly for making a profit, to take the custody of sensitive data, raises underlying security and privacy issues. In this paper we propose an efficient, secure and privacy preserving keyword search scheme which supports multiple users with low computation cost and flexible key management and it is proved to be secure and flexible.*

Key Words: **Cloud Storage Services; Security; Searchable Encryption; Partial decipherment; Privacy Preserving**.

1. INTRODUCTION

Cloud computing is one of the top 10 strategic technologies, dynamically provides high-quality cloud based services and applications over the Internet. Cloud Computing, in which enterprise's or individual's databases and applications are moved to the servers in the large data centers (i.e. the cloud) managed by the third-party cloud service providers (CSPs) in the Internet. People are fascinated by the benefits offered by cloud, such as ubiquitous and flexible access, on-demand computing resources configuration, considerable capital expenditure savings, etc. Indeed, many companies, organizations, and individual users have adopted the cloud platform to facilitate their business operations, research, or everyday needs.

Cloud computing constitutes a large computing resources pool which can provide service to users on their demand. Cloud Storage Services Provides the large space of data storage resources and it stores the data on the remote servers based on the Cloud Computing. It includes database-like services and network attached storage. The main purpose of using these services is outsourcing the data. Using this we can access the data from anywhere in the word by any devices that is connected to the network. So it provides the biggest flexibility. For Example the user can store the file or some documents on the Cloud Storage. Now after some time it want to retrieve this then it uses some keywords that define in that file. So user sends keyword to CSP. The CSP checks and finds this keyword and sends appropriate output to the user. So in this process the keyword must be secure from unauthorized user. For this task it decrypts the all documents. For above example if any unauthorized person knows user keyword than that person sends the request for searching this keyword specific document as a legal request. Than easily it gets the same results and shows the user private data. To avoid this problem we can use the some natural approached like searchable encryption scheme. Now in this paper, we propose an efficient encrypted keyword search scheme suitable for Cloud Storage.

In this secure and privacy preserving search keyword on encrypted data approach contains three participants are there: 1) user 2) key server 3)CSP. CSP contains many schemas that use the system models like Public key encryption with keyword searching (PKES), Efficient and Privacy Preserving Keyword Search (EPPKS) and Secure and Privacy Preserving Keyword Search (SPKS).These types of the schemas generally use the following function in the given order:

1. Key Generation
2. Email Encryption
3. Keywords Encryption
4. Trapdoor Computing
5. Testing
6. Decryption/Partial Decryption
7. Recovery

The goal of this schema is: The document stored in cloud storage is not accessed by an unauthorized user. It also used to avoid the statistical attack on the cloud storage. This searchable encryption scheme has the following advantages:

a. It supports keyword search in encrypted form. The Cloud Server could determine which all documents contain the specified keyword without knowing anything about the contents of document or the keyword searched.

b. The service provider will participate in the partial decipherment of the cipher text, thus reducing them computational overhead of the user.

c. Same keywords are encrypted to different cipher text for different documents thus reducing redundancy and avoiding the chance of statistical attack on keyword cipher text. So for that every time random key is generated.

II Related Work

It is an important question is that how to Cloud Service Provider to efficiently search the keyword in encrypted form on encrypted files and providing user data privacy at the same time. The question was first raised in Song et al. (2000). Since then, there has been much work conducted in this field, such as Haclgiimfi et al. (2002), Boneh et al. (2004), Chang and Mitzenmacher (2005), Boneh and Waters (2007), Shi et al. (2007), and Liu et al. (2009). Boneh et al. (2004) proposed a public key encryption with keyword searching (PEKS) scheme, which supports encrypted keyword search. Here the document is encrypted with any public key encryption algorithm and the user needs to decrypt it completely by him. So it will use too much CPU and memory power of the client if documents are decrypted frequently and loose the critical value of Cloud Computing.

In our previous work (Liu et al., 2009), to allow users to efficiently access files containing certain keywords in a cloud anytime and anywhere using any device, we proposed an efficient privacy preserving keyword searching scheme (EPPKS) in cloud computing by making performance improvements to the PEKS scheme. Inspired by the work of Diament et al. (2004).This scheme allows the service provider to participate in partial decipherment of the searched documents thus reducing the computational overhead of the user. In this scheme if the keyword encryption uses public key of all share users then that is used for multi user also. In multi user approach, the trapdoor is made as the keyword query with the partial of every computed public key. When the number of users increases, it has low efficiency and it is not so efficient for the actual application of Cloud. For this proposed a scheme shared and searchable encrypted data for untrusted servers. It supports multiple users. In this case encryption is not based on public key. In this scheme service provider performs partial decryption. But it can't resist the statistical attack on keywords. Here same keyword is encrypted to same cipher texts only for different documents.

III. BASIC SYSTEM MODEL

In this Privacy Preserving Encrypted Keyword Search Scheme there are three participants.

1] User: Users are the authorized person that stores the file, update the file, and operate some functions like encryption decryption.

2] Key Server: Key server is a trusted server which stores all the keys used for encrypting the document along with the signature of file names. The key server provides the key for decrypting a file to the user after verifying the signature of file name.

3]CSP: The data centre who provides the storage service. The users stored the cipher text of their file, the cipher text of the metadata of the files and the cipher text of the keyword into the Cloud Storage Server, so that the server can know nothing about the information in the files and keywords.

The basic mode of this approach is described in following Figure 1.

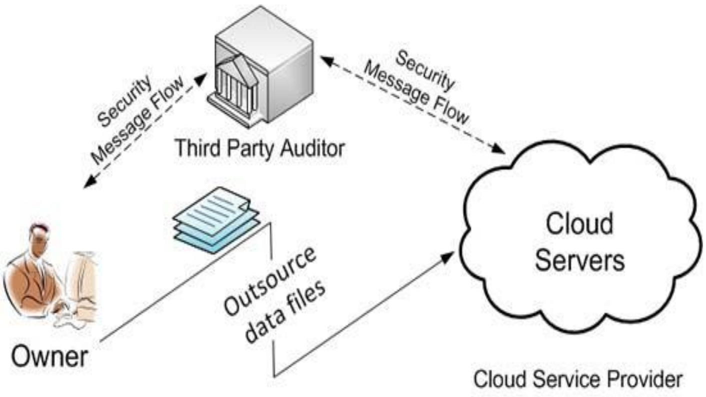

Fig -1: Secure Cloud Storage Basic System Model

IV. VARIOUS SCHEMAS

There are many different schemas are available that are described below.

1] Public Key Encryption with Keyword Searching (PEKS):

It is an asymmetric searchable encryption scheme, where encryption is done using a public key system. This was designed for the purpose of intelligent email routing. In this scheme, when a user requests a particular keyword, the server should retrieve the files or mails, which are in the server, but the server, should not know anything about the mail or the keyword. The four algorithms that are in this technique are given below:

a. **A Receiver Key Generation Algorithm KeyGenReceiver (k):** Taking a security parameter k ∈ IN as input, this algorithm generates a private and public key pair (skR, pkR) of the receiver. Note that pkR includes the security parameter, descriptions of a finite keyword space and a PEKS cipher text space.

b. A **PEKS Algorithm PEKS (pkR, w):** Taking a receiver's public key pkR and a keyword w as input, this algorithm generates a PEKS cipher text S which is a searchable encryption of w. We write S = PEKS (pkR, w).

c. **A Trapdoor Generation Algorithm Trapdoor (skR, w):** Taking a receiver's private key skR and a keyword w as input, this algorithm generates a trapdoor Tw for the keyword w.

d. **A Test Algorithm Test (Tw, S):** Taking a trapdoor Tw for a keyword w and a PEKS ciphertext S =

PEKS(pk, w0), this algorithm returns a symbol "Correct" if w = w 0 and "Incorrect" otherwise.

In the following figure this applied by following way. 1) If Alice and Bob are the same User 'U' want to store its document on the CSP then first it runs the Key generation algorithm to generate the private and public key. 2) Now it uses the searchable encryption algorithm or PEKS for encrypting the document and respectively keywords. 3) Now 'U' wants to retrieve this document that containing the keyword W then runs the Trapdoor algorithm to compute Trapdoor for W and sends to CSP. 4) After receiving trapdoor the CSP uses the Test function for finding documents that contains same keyword.

The working process of this is described in Figure 2.

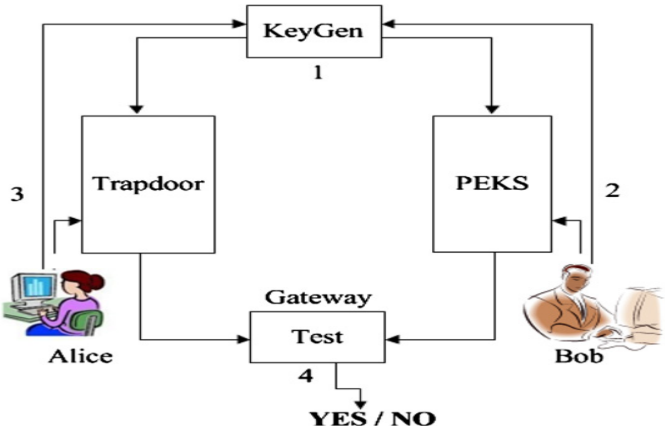

Figure-2: The working process of the PEKS scheme

2] **Efficient and Privacy Preserving Keyword Search (EPPKS):**

When the encryption is not searchable the service provider will not be able to know which files are containing the keywords that are requested by the user. In this situation, the service provider will return all the encrypted files. If the user is using a thin client with a limited bandwidth, it will not be able to handle such situations, because of its limited bandwidth and memory. So this schema used the partial decipherment, which will reduce the client's computational overhead, and enable the service provider to search through the encrypted files for the requested keywords in order to protect the user data privacy. Seven randomized polynomial time algorithms are used here, they consists of the following,

a. ***Key Generation:***

It takes large security parameter K1 and generates the public key pair for user kwon as (Upub, Upriv). Now also take another large security parameter K2 and generate another public key pair for CSP known as (Spub, Spriv).

b. ***Email Encryption (EMBEnc):***

It uses the public key encryption algorithm.It takes two key Upub, Spub and message M as a input and encrypt the message that known as Cm. So We write EMBEnc (Upub; S pub;m) = Cm.

c. ***Keyword Encryption (KWEnc):***

It is also performs the public key encryption algorithm. It takes the public key Upub and keyword Wi Є W (i Є Z+) as a input and produces cipher text CWi's Є CW. So we can write KWEnc(Upub;Wi) = CWi .

d. ***Trapdoor Computing (TCompute):***

It takes the Upriv key and keyword like Wj Є W (j Є Z+) as a input and generate the Wj's trapdoor known as TWj. So we can write TCompute(Upriv, Wj) = TWj.

e. ***Testing:***

Now it uses the CWi, TWj and Upub as a input and checks the finding keyword. It returns 1 if CWi=TWj otherwise it returns 0.

f. ***Decryption:***

It takes Upub, Spriv, and Cm as an input and generates the intermediate result Cp.

g. ***Recovery:***

It uses the Upriv to decrypt the Cp. So it takes Upriv and Cp as an input and generates the final output plain text M.

3] **Secure and Privacy Preserving Keyword Search (SPKS):**

The SPKS scheme enables the CPS's to participate in the partial decipherment, this will reduce the computational overhead on users, without leaking any information about the plain text. It also supports keyword searching on encrypted data. This scheme will enable the CSP to determine whether the keyword specified by the user is in the email, but it will not be aware of the information contained in the email, nor the keyword that was searched. It is proven to be semantically secure under the Bilinear Diffie Hellman assumption and the random oracle model. The working process of this schema is described in the following Figure 3.

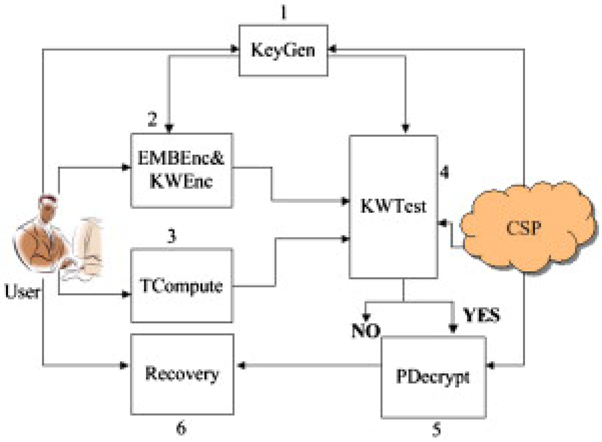

Figure-3: The working process of the SPKS scheme.

This scheme consists of seven randomized polynomial time algorithms. They are as follows:

a. **Key Generation**:

It takes large security parameter K1 and generates the public key pair for user kwon as (Upub,Upriv). Now also take another large security parameter K2 and generate another public key pair for CSP known as(Spub,Spriv).

b. Email Encryption (EMBEnc):

It uses the public key encryption algorithm. It takes two key Upub, Spub and message M as a input and encrypt the message that known as Cm. So We write EMBEnc (Upub; S pub;m) = Cm.

c. Keyword Encryption (KWEnc):

It is also performs the public key encryption algorithm. It takes the public key Upub and keyword Wi Є W (i Є Z+) as a input and produces cipher text CWi's Є CW. So we can write KWEnc(Upub;Wi) = CWi .

d. Trapdoor Computing (TCompute):

It takes the Upriv key and keyword like Wj Є W (j Є Z+) as a input and generate the Wj's trapdoor known as TWj. So we can write TCompute(Upriv, Wj) = TWj.

e. Testing:

Now it uses the CWi, TWj and Upub as a input and checks the finding keyword. It returns 1 if CWi=TWj otherwise it returns 0.

f. PDecryption:

It takes Upub, Spriv, and Cm as an input and generates the intermediate result Cp. We can write PDecrept(Upub, Spriv, Cm) = Cp.

g. Recovery:

It uses the Upriv to decrypt the Cp. So it takes Upriv and Cp as a input and generate the final output plain text M.

V. CONCLUSIONS

In this paper, we focus on the privacy concerns in the secure search function performed over encrypted cloud data. The study of different keyword searching schemes that offers a way to overcome one technique's disadvantage. The keyword searching techniques improve the security of the user keyword searching privacy. Now SPKS allows the CSP to participate in the decipherment, thus a user could pay less computational overhead for decryption. It is a searchable encryption scheme, thus the CSP could search the encrypted files efficiently without leaking any information. So from this various approaches like PEKS, SPKS etc, the SPKS is more efficient and privacy preserving keyword search schema.

REFERENCES

[1] Ms. Pooja D. Shah and Mr. Gopal Pandey,"Privacy Preserving Keyword Search for Encrypted Cloud Storage Data" International Conference on "Advance Computing and Creating Entrepreneurs (ACCE2013)" On 19-20 Feb 2013.

[2] Qin Liu, Guojun Wang, Jie Wu," Secure and privacy preserving keyword searching for cloud storage services" Journal of Network and Computer Applications on 2011.

[3] Joonsang Baek, Reihaneh Safiavi-Naini,Willy Susilo," Public Key Encryption with Keyword Search Revisited".

[4] Qin Liu, Guojun Wang, and Jie Wu," An Efficient Privacy Preserving Keyword Search Scheme in Cloud Computing".

[5] Seny Kamara and Kristin Lauter, "Cryptographic Cloud Storage," Microsoft research.

[6] Tritty Mamachan1, and Roshni. M. Thankar, "Survey on keyword searching in Cloud Storages," International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 2, Issue 11, November 2012.

[7] Liu Hong-xia, Dai Jia-zhu, and Jiang Chao, "Research on Privacy Preserving Keyword Search in Cloud Storage," IEEE publication, 978-1-4244-5540- 9/10, 2010.

[8] Qin Liuy, Guojun Wang, and Jie Wuz, "An Efficient Privacy Preserving Keyword Search Scheme in Cloud Computing," Computational Science and Engginerring, IEEE publication, 29-31 Aug 2009.

[9] Qin Liuy, Guojun Wang, and Jie Wuz, "Secure and privacy preserving keyword searching for Cloud Storage Services," Journal of Network and Computer Applications, 9 March 2011.