AN ANALYSIS OF FILE SECURITY ON CLOUD USING 'DUAL SERVER ENCRYPTION' AND SUGGESTION OF KEYWORD SEARCH IN PUBLIC KEY ENCRYPTED FILES TO ENHANCE SECURITY

Atul Kalkhanda

ABSTRACT

Cloud computing is nowadays becoming a hot topic. A number of companies are using cloud services for data storage and data security. Cloud is made up of several servers connected in a network, and are placed in different regions. This architecture is designed in such a way that authentic users can easily store, read, and write data from a remote device. Till the present day, there are few or no provisions to store files securely in the public and private cloud. In this research, it has been endeavored to focus on the different security techniques and levels. For this keyword search in public key encrypted files may be used and has been suggested..

INTRODUCTION

In recent days, the cloud server has got a user's attention towards storing and reading data. As the data is being increasing day by day, almost all the companies are unable to store their valuable data on their devices, so in this situation, they opt for a new data storage location known as Cloud Data Storage. Generally, the data which is saved on the server is commonly used for sharing within the users of the same group or between the users of different groups with valid authentication. Google Drive, Drive Hq Server, DropBox, and ICloud are Some of the best cloud data storage services which are widely used in day to day life.

MAIN CONTRIBUTIONS FOR DOING THIS PROPOSED WORK

The main contribution for doing this proposed paper contains four main reasons like:

1. At first, we are proposing a KSPKE technique named Two Phased-Server Public KSPKE to address the security vulnerability of primitive KSPKE which is already proposed in the literature.

2. Designing a generic SPHF, referred to as linear and homomorphic KSPKE.

3. Next we try to show a generic construction of KSPKE.

4. To illustrate the feasibility of this novel framework, an efficient instantiation of Linear-Homomorphic SPHF.

BACKGROUND WORK

In this section we are focusing on our proposed system performance i.e. KSPKE

2.1.1 MAIN MOTIVATION

In this section, we will initially try to find out the system model and assumptions that were used in the current paper. Now let us look about them in detail:

Traditional PEKS: A well-known authors like Boneh and another well-known author like Abdalla mainly constructed the anonymous IBE (also known as AIBE), and they try to design a novel searchable encryption from AIBE. In this study, they mainly try to construct a hierarchical IBE (HIBE) scheme into well-known public-key encryption with a temporary keyword search (PETKS).

PROPOSED NOVEL DUAL-SERVER PUBLIC KEY ENCRYPTION WITH KEYWORD SEARCH USING SMOOTH PROJECTION HASHING (DS-PEKS)

In this section, we will find out the proposed novel KSPKE protocol that was used in the current thesis in order to give a high level of security for the sensitive data which is stored and accessed to and from the cloud server.

- $\mathsf{Setup}(1^{\lambda})$. *Takes as input the security parameter* λ, *generates the system parameters* P;
- $\mathsf{KeyGen}(P)$. *Takes as input the systems parameters* P, *outputs the public/secret key pairs* (pk_{FS}, sk_{FS}), *and* (pk_{BS}, sk_{BS}) *for the front server, and the back server respectively;*
- $\mathsf{DS-PEKS}(P, pk_{FS}, pk_{BS}, kw_1)$. *Takes as input* P, *the front server's public key* pk_{FS}, *the back server's public key* pk_{BS} *and the keyword* kw_1, *outputs the PEKS ciphertext* CT_{kw_1} *of* kw_1;
- $\mathsf{DS-Trapdoor}(P, pk_{FS}, pk_{BS}, kw_2)$. *Takes as input* P, *the front server's public key* pk_{FS}, *the back server's public key* pk_{BS} *and the keyword* kw_2, *outputs the trapdoor* T_{kw_2};
- $\mathsf{FrontTest}(P, sk_{FS}, CT_{kw_1}, T_{kw_2})$. *Takes as input* P, *the front server's secret key* sk_{FS}, *the PEKS ciphertext* CT_{kw_1} *and the trapdoor* T_{kw_2}, *outputs the internal testing-state* C_{ITS};
- $\mathsf{BackTest}(P, sk_{BS}, C_{ITS})$. *Takes as input* P, *the back server's secret key* sk_{BS} *and the internal testing-state* C_{ITS}, *outputs the testing result 0 or 1;*

Correctness. It is required that for any keyword kw_1, kw_2, and $CT_{kw_1} \leftarrow \mathsf{DS-PEKS}(P, pk_{FS}, pk_{BS}, kw_1)$, $T_{kw_2} \leftarrow \mathsf{DS-Trapdoor}(P, pk_{FS}, pk_{BS}, kw_2)$, we have

$$\mathsf{BackTest}(P, sk_{BS}, C_{ITS}) = \begin{cases} 1 & kw_1 = kw_2, \\ 0 & kw_1 \neq kw_2. \end{cases}$$

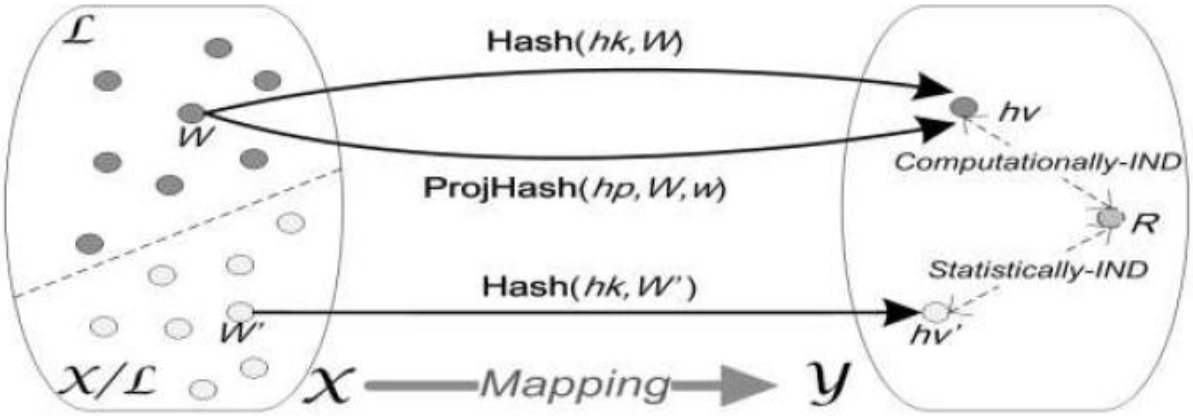
SPHF

This is the principal component for the development of double server open key encryption with watchword search, and the idea is spoken to as smooth projective hash work (SPHF), by two surely understood creators like Cramer and Shoup. Here we can examine the first meaning of a SPHF in the beneath sections.

From the above figure 1, we can clearly represent the architecture flow of an SPHF. Here we assume the domain with X and an NP language problem with L, where L contains a subset of the elements of the domain X, i.e., $L \subset X$. Formally, an SPHF system over a language $L \subset X$, onto a set Y, is defined by the following five attributes:

They are as follows:

SPHFSetup (1λ): generates the global parameters param and the description of an NP language instance L.
HashKG(L, param): generates a hashing key hk for L.
ProjKG$(\text{hk}, (L, \text{param}))$: derives the projection key hp from the hashing key hk.
Hash$(\text{hk}, (L, \text{param}), W)$: outputs the hash value hv $\in Y$ for the word W from the hashing key hk.
ProjHash$(\text{hp}, (L, \text{param}), W, w)$: outputs the hash value hv1 $\in Y$ for the word W from the projection key hp and the witness w for the fact that $W \in L$.
The *correctness* of an SPHF requires that for a word $W \in L$ with w the witness,



RESULT ANALYSIS

In this section, we mainly describe the result in the analysis of the cease of our utility. Here we can see the server window that represents that server can view all of the document details alongside a set of personal details and additionally the requests that became raised by using the cease customers. Here the customers can connect to this centralized server to have access to the documents to and from the cloud server. From the below window, we can surely find out that the statistics user gets get admission to keys from the servers so as for making the record downloaded into the laptop in a usual text manner. For this, he wants to request the two servers, in my opinion, and if the two servers the first server and returned server offers approval for statistics download, then only he can download the data in an understandable text manner. If any of the keys is not obtained for the data person, he/she cannot capable of getting the right of entry to the data, and they are able to able to view the records in a usual text manner

CONCLUSION

In our research, we have proposed a novel approach i.e., keyword-based public-key encryption that helps in protecting sensitive files from outsiders or hackers.