**STRENGTHENING CLOUD COMPUTING SECURITY: MECHANISMS FOR SECURE KEYWORD SEARCH AND DATA SHARING**

**Abstract:**

The emergence of cloud infrastructure has significantly reduced the costs of hardware and software resources in computing infrastructure. To ensure security, the data is usually encrypted before it’s outsourced to the cloud. Unlike searching and sharing the plain data, it is challenging to search and share the data after encryption. Nevertheless, it is a critical task for the cloud service provider as the users expect the cloud to conduct a quick search and return the result without losing data confidentiality. To overcome these problems, we propose a cipher text-policy attribute-based mechanism with keyword search and data sharing (CPAB-KSDS) for encrypted cloud data. The proposed solution not only supports attribute-based keyword search but also enables attribute-based data sharing at the same time, which is in contrast to the existing solutions that only support either one of two features. Additionally, the keyword in our scheme can be updated during the sharing phase without interacting with the PKG. In this paper, we describe the notion of CPAB-KSDS as well as its security model. Besides, we propose a concrete scheme and prove that it is against chosen cipher text attack and chosen keyword attack secure in the random oracle model. Finally, the proposed construction is demonstrated practical and efficient in the performance and property comparison.

**Existing System:**

The traditional attribute-based encryption is not flexible for data searching and sharing. Additionally, attribute-based encryption is not well scaled when there is an update request to the keyword. In order to search and share a specific record, Alice downloads and decrypts the cipher texts. However, this process is impractical to Alice especially when there are a tremendous number of cipher texts. The worse situation is the data owner Alice should stay online all the time because Alice needs to provide her private key for the data decryption. Thus, ABE solution does not take the advantages of cloud computing.

An alternative method is to delegate a third party to do the search, re-encrypt and keyword update work instead of Alice. Alice can store her private key in the third party’s storage, and thus the third party can do the heavy job on behalf of Alice. In such an approach, however, we need to fully trust the third party since it can access to Alice’s private key. If the third party is compromised, all the user data including sensitive privacy will be leaked as well. It would be a severe disaster to the users.

**Disadvantages:**

1. To ensure security, the data is usually encrypted before it's outsourced to the cloud. Unlike searching and sharing the plain data, it is challenging to search and share the data after encryption.

2. Nevertheless, it is a critical task for the cloud service provider as the users expect the cloud to conduct a quick search and return the result without losing data confidentiality.

**Proposed System:**

Prior work did not demonstrate that the existing attribute-based mechanisms could both support keyword search and data sharing in one scheme without resorting to PKG. Therefore, a new attribute-based mechanism is needed to achieve the goal for the above PHR scenario. One may argue that the problem can be trivially solved by combining an AB-PRE scheme and attribute-based keyword search scheme (AB-KS).However, the combination could result in two major issues: 1) the combined scheme is not CCA secure, 2) it is vulnerable to collusion attack

Therefore, a secure scheme is desired to fully support keyword searching, data sharing as well as the protection ofthe privacy of keyword. All of these concerns motivate us to design a mechanism that:

1) Allows the data owner to search and share the encrypted health report without the unnecessary decryption process.

2) Supports keyword updating during the data sharing phase.

3) More importantly, does not need the exist of the PKG, either in the phase of data sharing or keyword updating.

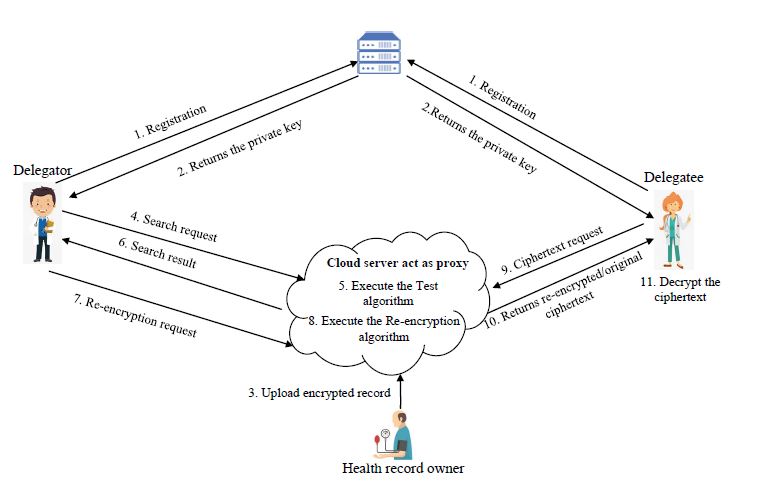
We first introduce a cipher text-policy attribute-based mechanism with keyword search and data sharing (CPAB-KSDS) for encrypted cloud data. The searching and sharing functionality are enabled in the cipher text-policy setting. Furthermore, our scheme supports the keyword to be updated during the sharing phase. After presenting the construction of our mechanism, we proof its chosen cipher text attack (CCA) and chosen keyword attack (CKA) security in the random oracle model. The proposed construction is demonstrated practical and efficient in the performance and property comparison.

**Advantages:**

1. We describe the notion of CPAB-KSDS as well as its security model.

2. The proposed construction is demonstrated practical and efficient in the performance and property comparison.

**System Architecture**:



**MODULES**

1. System Initialization
2. Registration
3. Ciphertext Upload
4. Ciphertext Search
5. Re-encryption
6. Decryption

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* PROCESSOR :I3.
* Hard Disk : 40 GB.
* Ram : 2 GB.

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows.
* Coding Language : JAVA/J2EE
* Data Base : MYSQL
* IDE : Netbeans8.1
* Server : Apache Tomcat