**Privacy Preserving Computation with Flexible Access Control Using Cloud Data**

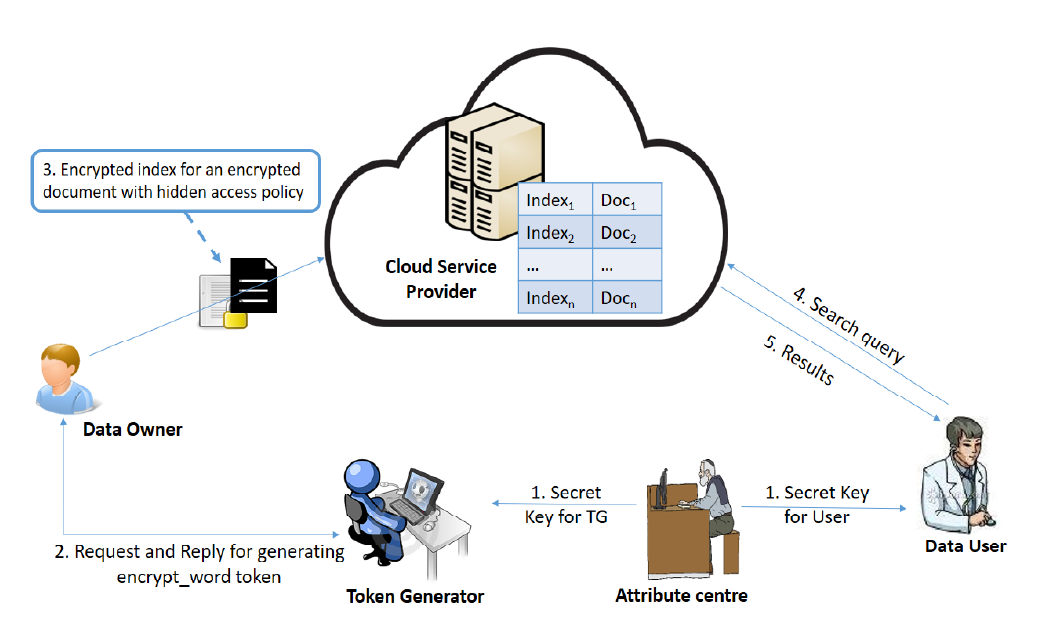
**ABSTRACT:-**

Searchable encryption facilitates cloud server to search over encrypted data without decrypting the data. Single keyword based searchable encryption enables a user to access a subset of documents, which contains the keyword of the user’s interest. In this paper, we present a single keyword based searchable encryption scheme for the applications where multiple data owners upload their data and then multiple users can access the data. The scheme uses attribute based encryption that allows user to access the selective subset of data from cloud without revealing his/her access rights to the cloud server. The scheme is proven adaptively secure against chosen-keyword attack in the random oracle model. We have implemented the scheme on Google cloud instance and the performance of the scheme found practical in real-world applications.

|  |  |
| --- | --- |
| **EXSISTING SYSTEM** | **PROPOSED SYSTEM** |
| * The scope of the PSE scheme is to generate the index of encrypted keywords for a document and to perform privacy preserving search over the encrypted index. * It does not include the encryption and decryption of a document. * An existing efficient AABE scheme can be used for the encryption and decryption of a document. | * We present a privacy preserving single keyword-based searchable encryption scheme (PSE) with fine-grained access control. * The scheme is designed with multi-sender and multi-receiver setup, aimed at facilitating a data owner (sender) to encrypt the index of keywords related to his document and uploads it along with the access policy and the encrypted document on cloud storage, where the access policy is decided by the data owner and kept hidden inside the ciphertext. * The user(receiver) sends his search query in the form of trapdoor to the cloud storage server. |
| **EXISTING ALGORITHM**  Authorized Searchable Public-Key Encryption (ASPKE) | **PROPOSED ALGORITHM**  Privacy Preserving Single Keyword-Based Searchable Encryption Scheme (PSE) |
| **ALGORITHM DEFINITION:-**  Searchable public key encryption (SPE) that supports multi-keywords search, allows data users to retrieve encrypted files of interest efficiently, and thus it has been intensively studied during recent | **ALGORITHM DEFINITION:-**  Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both the encryption of plaintext and the decryption of ciphertext. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. |
| **DRAWBACKS:-**   * These schemes do not address the important issue of receiver anonymity. * The user has to acquire the search token from the trusted authority, which increases the per query interaction overhead for search operation on user side. | **ADVANTAGES:-**   * The proposed PSE scheme provides a keyword based search facility over attribute based encrypted data with hidden access policy. * The scheme is applicable in a scenario where there are multiple data owners and multiple data receivers |

**System model with a cloud server, a data owner and**

**data users.**

****

**MINIMUMSYSTEM REQUIREMENTS**

**HARDWARE REQUIREMENTS**

* PROCESSOR : DUAL CORE 2 DUO.
* RAM : 2GB DD RAM
* HARD DISK : 250 GB

**SOFTWARE REQUIREMENTS**

* FRONT END : J2EE (JSP, SERVLET)
* BACK END : MY SQL 5.5
* OPERATING SYSTEM : WINDOWS 7
* IDE : ECLIPSE