**OUTSOURCED ATTRIBUTE BASED ENCRYPTION WITH KEYWORD SEARCH FUNCTION FOR CLOUD STORAGE**

**ABSTRACT:**

Cloud computing becomes increasingly popular for data owners to outsource their data to public cloud servers while allowing intended data users to retrieve these data stored in cloud. This kind of computing model brings challenges to the security and privacy of data stored in cloud. Attribute-based encryption (ABE) technology has been used to design fine-grained access control system, which provides one good method to solve the security issues in cloud setting. However, the computation cost and cipher text size in most ABE schemes grow with the complexity of the access policy. Outsourced ABE (OABE) with fine-grained access control system can largely reduce the computation cost for users who want to access encrypted data stored in cloud by outsourcing the heavy computation to cloud service provider (CSP). However, as the amount of encrypted files stored in cloud is becoming very huge, which will hinder efficient query processing? To deal with above problem, we present a new cryptographic primitive called attribute-based encryption scheme with outsourcing key-issuing and outsourcing decryption, which can implement keyword search function (KSF-OABE). The proposed KSF-OABE scheme is proved secure against chosen-plaintext attack (CPA). CSP performs partial decryption task delegated by data user without knowing anything about the plaintext. Moreover, the CSP can perform encrypted keyword search without knowing anything about the keywords embedded in trapdoor. Here we used the algorithm is,

* Set-up Algorithm

Architecture diagram:



EXISTING SYSTEM:

Out Sourced Attribute Based Encryption with Keyword Search Function for Cloud Storage, In this case, the File key can be uploading based on the attribute functions. The file can be uploading if the authorized person gives a key to upload a file. If a group is updated, then the group key changes to the shared key of the new group.

The drawback of is that the user key size is combinatorial large in the total number of users (if the system is unconditionally secure).Another drawback is that the group key of a given group cannot be changed even if it is leaked unexpectedly (e.g.) cryptanalysis of cipher texts bearing this key).The key size problem may be overcome if a computationally secure easy. Further, computationally secure KPS is only known for the two party cases and the three-party case KPs with a group size greater than still open.

**Disadvantages:**

1. The User key size is combinational large in the total number of users (if the system is unconditionally secure).

2. The given key can not be changed even if it is leaked unexpectedly.

**Proposed system:**

The out sourced attribute based encryption with keyword search function for cloud storage with an arbitrary connectivity graph, where each user is only aware of his neighbors and has no information about the existence of other users.

Further, he has no information about the network topology. Under this setting a user does not need to trust a user who is not his neighbor.

Thus, if one is initialized using PKI, then the need not trust or remember public keys of users beyond his neighbours.

**Advantages:**

1. To update the key more efficiently than just running the protocol again, when user memberships are changing.

2. Two passively secure protocols with contributiveness and proved lower bounds on a round complexity, demonstrating that our protocols are round efficient.

**MODULES:**

In our Project we are using five modules. The Modules are,

* + - Trusted Authority (TA).
    - Key Generation Cloud Service Provider (KG-CSP).
    - Decryption-Cloud Service Provider
    - (D-CSP).
    - Storage-Cloud ServiceProvider (S-CSP).
    - Data Owner (DO).

**Trusted Authority (TA).**

TA is the attribute authority center, which is responsible for the initialization of system parameters, and the generation of attribute private keys and trapdoor.

**Key Generation Cloud Service Provider (KG-CSP).**

It a participant that supplies outsourcing computing service for TA by completing the costly key generation tasks allocated by TA.

**Decryption-Cloud Service Provider (D-CSP).**

It is a participant that supplies outsourcing computing service through accomplishing partial decryption for cipher texts and keyword search service on the partially decrypted cipher texts for data users who want to access the cipher text.

**Storage-Cloud ServiceProvider (S-CSP).**

It is a participant that supplies out sourcing data storage service for users who want to share file in cloud.

**Data Owner (DO).**

This is a participant who intends to upload and share his data files on the cloud storage system in a secure way. The encrypted cipher texts will be shared with intended receivers whose access structure will be satisfied by attribute set embedded in cipher texts, that is to say the predicate . The responsibility of DO is to generate indexes for some keywords and upload encrypted data with the indexes.

**Data User (DU).**

This is a participant who decrypts the encrypted data stored in S-CSP with the help of D-CSP. If the attribute set for DU satisfies the access structures, DU is able to access the encrypted files and recover the original files from it. DU downloads intended cipher texts with the help of trapdoor associated with appointed keyword. Data user is responsible for choosing keywords to create trapdoor, and decrypting data.

# H/W System Configuration:-

# Processor - Pentium –IV

**Speed - 2.69 Ghz**

**RAM - 1GB(min)**

**Hard Disk - 500 GB**

**Key Board - Standard Windows Keyboard**

**Mouse - Two or Three Button Mouse**

**Monitor - LCD/LED monitors**

# S/W System Configuration:-

* Operating System :Windows XP/7
* Front End : java, jdk1.8
* Database : My sqlserver
* Database Connectivity : JDBC.

**CONCLUSION:**

In this project, we propose a CP-ABE scheme that provides outsourcing key-issuing, decryption and keyword search function. Our scheme is efficient since we only need to download the partial decryption ciphertext corresponding to a specific keyword. In our scheme, the time-consumingpairing operation can be outsourced to the cloud service provider, while the slight operations can be done by users. Thus, the computation costat both users and trusted authority sides is minimized. Furthermore, the proposed scheme supports the function of keywords search which can greatly improve communication efficiency and further protect the security and privacy of users. Actually, we are easy to extend our KSF-OABE scheme to support access structure represented by tree.