**IMPLEMENTATION**

**MODULES:-**

* **Key generation centre (KGC)**.
* **Cloud server (CS)**.
* **Data owner**.
* **Data user**.

**MODULES DESCRIPTION:-**

**Key generation centre (KGC):**

KGC is responsible to generate the public parameter for the system and the public/secret key pairs for the users. Once the user’s secret key is leaked for profits or other purposes, KGC runs trace algorithm to find the malicious user. After the traitor is traced, KGC sends user revocation request to cloud server to revoke the user’s search privilege.

**Cloud server (CS):**

Cloud server has tremendous storage space and powerful computing capability, which provides on-demand service to the system. Cloud server is responsible to store the data owner’s encrypted files and respond on data user’s search query.

**Data owner:**

Data owner utilizes the cloud storage service to store the files. Before the data outsourcing, the data owner extracts keyword set from the file and encrypts it into secure index. The document is also encrypted to ciphertext. During the encryption process, the access policy is specified and embedded into the ciphertext to realize finegrained access control.

**Data user:**

Each data user has attribute set to describe his characteristics, such as professor, computer science college, dean, etc. The attribute set is embedded into user’s secret key. Using the secret key, data user is able to search on the encrypted files stored in the cloud, i.e., chooses a keyword set that he wants to search. Then, the keyword is encrypted to a trapdoor using user’s secret key. If the user’s attribute set satisfies the access policy defined in the encrypted files, the cloud server responds on user’s search query and finds the match files. Otherwise, the search query is rejected. After the match files are returned, the user runs decryption algorithm to recover the plaintext.