**IMPLEMENTATION**

* **Data Owner Module**

In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the data file and then store in the cloud. The data owner can check the duplication of the file over Corresponding cloud server. The Data owner can have capable of manipulating the encrypted data file and the data owner can check the multiple cloud data as well as the duplication of the specific file. And also he can create remote user with respect to registered cloud servers. And also data owner has migrate to another cloud option, by this he can migrate files from one cloud server to another cloud server.

* **Connector Module**

In this module, the connector helps to check duplication of file existed or not in cloud server and you can check in multi cloud servers also. If it is existed then also owner trying to upload the same file in same cloud server then connector automatically blocks his access permission. If it is not existed then data owner can upload file in multi cloud servers at a time.

* **Cloud Server Module**

The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with Remote User. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them.

* **Remote User**

In this module, remote user logs in by using his user name and password. After he will request for secrete key of required file from cloud servers, and get the secrete key. After getting secrete key he is trying to download file by entering file name and secrete key from cloud server.

* **Data Encryption and Decryption**

All the legal users in the system can freely query any interested encrypted and decrypted data. Upon receiving the data from the server, the user runs the decryption algorithm Decrypt to decrypt the cipher text by using its secret keys from different Users. Only the attributes the user possesses satisfy the access structure defined in the cipher text CT, the user can get the content key.

* **Attacker Module**

In remote user module, while downloading time if remote user entered any wrong file name or secrete key then cloud servers treats him as attacker and moves his access permission to block/attacker list.