**IMPLEMENTATION**

* **Data Owner**

In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the file and then store in the cloud. The data owner can have capable of updating and deleting of a specific file. And also he can view the transactions based on the files he uploaded to cloud.

* **End User**

In this module, receivers logs in by using his/her user name and password. After Login receiver will Search for files and request for secret key of a particular file from Authority, and get the secret key. After getting secret key he is trying to download file by entering file name and secret key from cloud server.

* **Authority**

In this module, the authority helps to check transaction of files and also. If receiver exists and the profile. Authority also view the requests from the receivers and generates the secret key and send to the requested data receivers.

* **Cloud Server**

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.

* **Data Encryption and Decryption**

All the legal receivers in the system can freely query any interested encrypted and decrypted data. Upon receiving the data from the server, the receiver runs the decryption algorithm Decrypt to decrypt the cipher text by using its secret keys from different Users.

* **Attacker Module**

In Data Receiver module, while downloading files if receiver enters wrong secret key for particular file, then cloud servers treats him as attacker and moves to attacker list.