Implementation

* **Data owner**

In this module, the data owner should register by providing user name, password, email and group, after registering owner has to Login by using valid user name and password. The Data owner browses and uploads their data to the cloud server. For the security purpose the data provider encrypts the data file and then stores in the web server.

* **Group Authority**

The group authority is responsible for registering and login authorization for   
 the end users if they are in the same group and also 1. View Group Users 2.   
 View Group Signs 3. View Registered User.

* **Storage Server** The Storage server is responsible for data storage and file authorization for an end user. The data file will be stored in cloud server with their tags such as Owner, file name, secret key, mac and private key, can also view the registered Owners and End-users in the cloud server. The data file will be sending based on the privileges. If the privilege is correct then the data will be sent to the corresponding user and also will check the file name, end user name and secret key. If all are true then it will send to the corresponding user or he will be captured as attacker.
* **Data Consumer(End User)**

The data consumer is nothing but the end user who will request and gets file contents response from the corresponding cloud servers. If the file name and secret key, access permission like Search and download is correct then the end is getting the file response from the cloud or else he will be considered as an attacker and also he will be blocked in corresponding cloud. If he wants to access the file after blocking he wants to UN block from the cloud.

* **Attacker**

Threat model is one who is trying to receive files by giving fake Skey to the file in the Storage Server. The attacker may be within a Network or from outside the network. If attacker is from inside the network then those attackers are called as internal attackers. If the attacker is from outside the network then those attackers are called as external attackers.