**IMPLEMENTATION**

* **Data Owner Module**

In this module, the data owner uploads their data in the public cloud server. For the security purpose the data owner encrypts the data file and assigns the digital sign and then store in the cloud. The data owner can check the data integrity of the file over Corresponding cloud server. The Data owner can have capable of manipulating the encrypted data file and data owner can update the file contents as well as delete his own file.

* **Key Generation Centre**

In this module, the KGC Generates the Secret Key requested by the data user, the KGC checks the file if present generates the appropriate Secret Key. The KG-CSP allows viewing the Secret Key generated files and also the transactions related to the file.

* **Proxy Server**

The server will manage and authorize Users and maintain all data transactions between data owner and cloud server, end user.

* **Data User Module**

In this module, Data user logs in by using his user name and password. After he will request for secret key of required file from **CSP**, and get the secrete key from KGC. 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.

* **Attacker Module**

In Data user module, while downloading time if remote user enters wrong trapdoor or secrete key then he is treated as Digital sign attacker or Secret Key attacker.

* **Data Integrity Check**

Data will be verified in the cloud to check it is integrated by attacker or not. If it is integrated then it is recovering from the data owner.