**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’s blocks and then store in the cloud. The data owner can check the replication of the file’s blocks over Corresponding cloud server. The Data owner can have capable of manipulating the encrypted data file’s blocks and the data owner can check the cloud data as well as the replication of the specific file’s blocks and also he can create remote user with respect to registered cloud servers. The data owner also checks data integrity proof on which the block is modified by the attacker.

* **Cloud Server Module**

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

* **End 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’s blocks from cloud servers, and get the secrete key. After getting secrete key he is trying to download file’s blocks by entering file’s blocks 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**

The user who attacks or modifies the block content called attacker. The attacker may the user who tries to access the file contents by wrong secret key from the cloud server.