**IMPLEMENTATION**

### IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it’s constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

**MODULE DESCRIPTION:**

# Number of Modules

After careful analysis the system has been identified to have the following modules:

1. **Data owners**
2. **TPA**
3. **Cloud Server**
4. **Data Access Control**

# MODULES DESCRIPTION:

**Data Owners:**

The Data owner can register the first. While registering he required a valid user email and mobile for further communications. The owner can login into our system. After login the data owner can upload the file which is notepad readable file, because java IO classes can read only notepad readable files only. Select the data and encrypt it with symmetric key cryptography (i.e.AES-256 here). Update the Data Index List. It generates meta data of encrypted data using SHA-512 algorithm. Append encrypted data, data id and its public key. Encrypt these with RSA algorithm and send to CS.

**TPA:**

TPA can login with his credentials. Once he login he can challenge the data audit scheme. It decrypts the received challenge from DO. Append data id and its public key. Encrypted data can view by TPA. It decrypts the information sent by CS and recover the encrypted data. Calculate the message digest on received encrypted data. TPA requests for encrypted data to CS to check integrity. After that CS sends encrypted data to TPA. To protected data from an external attacker then CS has again encrypted the encrypted data to the public key. Because the key size is very increased then not affect the external attack.

**Cloud Server:**

CS can login with his credentials. Once he login he can view the data owners files and data audit information’s. It stores the encrypted data on its server and update its Data Access List. It decrypts the received challenge from TPA Append encrypted data, data id and its public key. Encrypt these with RSA algorithm and send to TPA. Send acknowledgement to DO. Store this new encrypted data on its server and updated the Data Access List.

**Data Access Control:**

The prospective method takes a data access list and data index list. The Data access-list essential contains the DID (Data ID) and BA (Base Address). This list only CS is performing operation and data index list contains DID. Only DO has the right to perform any operation. This list TPA is not access data. CS can store the encrypted data for the robust data access list. CS can forward encrypted data to TPA what is in their access rights.