**IMPLEMENTATION:**

**MODULES:**

* System Framework
* Data Owner
* Data User
* TPA
* Admin

**MODULES DESCRIPTION:**

**System Framework:**

The development of cloud computing and the popularity of smart mobile devices, people are gradually getting accustomed to a new era of data sharing model in which the data is stored on the cloud and the mobile devices are used to store/retrieve the data from the cloud. In these applications, people (data owners) can upload their documents and other files to the cloud and share these data with other people (data users) they like to share. CSPs also provide data management functionality for data owners. Since personal data files are sensitive, data owners are allowed to choose whether to make their data files public or can only be shared with specific data users. Clearly, data privacy of the personal sensitive data is a big concern for many data owners. We propose LDSS, a framework of lightweight data sharing scheme in mobile cloud. It has the following six components. (1)Data Owner (DO) (2) Data User (DU) (3) Trust Authority (TPA) (4) Encryption Service Provider (ESP) (5) Decryption Service Provider (DSP) (6) Cloud Service Provider (CSP).

**Data Owner (DO):**

When the data owner (DO) registers on TPA, TPA runs the algorithm Setup() to generate a public key PK and a master key MK. PK is sent to DO while MK is kept on TPA itself. DO defines its own attribute set and assigns attributes to its contacts. All these information will be sent to TPA and the cloud. TPA and the cloud receive the information and store it. DO uploads data to the mobile cloud and share it with friends. DO determines the access control policies. DO sends data to the cloud. Since the cloud is not credible, data has to be encrypted before it is uploaded. The DO defines access control policy in the form of access control tree on data files to assign which attributes a DU should obtain if he wants to access a certain data file.

**Data User (DU):**

DU logins onto the system and sends, an authorization request to TPA. The authorization request includes attribute keys (SK) which DU already has. TPA accepts the authorization request and checks the request and a generate attribute keys (SK) for DU. DU sends a request for data to the cloud.Cloud receives the request and checks if the DU meets the access requirement. DU receives the ciphertext, which includes ciphertext of data files and ciphertext of the symmetric key. DU decrypt the ciphertext of the symmetric key with the assistance of DSP. DU uses the symmetric key to decrypt the ciphertext of data files.

**Trusted Authority:**

A Third-Party Auditor (TPA) is introduced. It is responsible of generating public and private keys, and distributing attribute keys to users. With this mechanism, users can share and access data without being aware of the encryption and decryption operations. We assume TPA is entirely credible, and a trusted channel exists between the TPA and every user. The fact that a trusted channel exists doesn’t mean that the data can be shared through the trusted channel, for the data can be in a large amount. TPA is only used to transfer keys (in a small amount) securely between users. In addition, it’s requested that TPA is online all the time because data users may access data at any time and need TPA to update attribute keys.

**Admin:**

CSP stores the data for DO. It faithfully executes the operations requested by DO, while it may peek over data that DO has stored in the cloud. DU sends a request for data to the cloud. Cloud receives the request and checks if the DU meets the access requirement. If DU can’t meet the requirement, it refuses the request; otherwise it sends the ciphertext to DU. CSP manages the Uploaded Files.