

In File ID and Enc Key table, there are pairs of file id and its corresponding encryption key. PK\_A is stored in plaintext but the SK\_A is stored confidentially which is encrypted with password as the key. The above two structs compose the KMS of user A.

Shared with others table stores the file id and to whom it is shared.

Shared with me table stores the encrypted file’s id and corresponding key from others. The key for decrypting the file is encrypted with user A’s public key so A can decrypt them with own private key.

Login info includes the authentication information. Username is the only identity of every user and password is used in several procedure like authentication and de/encryption of own private key.

Log info records the operation of user.

Several operation procedures could be concluded as follows:



