CS628A: Computer Systems Security
Indian Institute of Technology Kanpur
Programming Assignment Number 1

Student: **Ankit Sharma(18111005), Deepak Yadav(18111015)**
Date: February 26, 2019

Review of Design Document(Hariom, Shikhar Barve)

1. User creation and authentication
   Rating - **2**
   - Design document does not mention how authentication of user is performed. No mention of implementation of InitUser and GetUser functions. There is Argon2(Username,Password) in username field but then how password is stored is unclear.

2. Integrity preservation in the simple secure client
   Rating - **2**
   - File's content integrity is not checked, it is only encrypted. Moreover, content of two UUIDs can be swapped and it will not detected.

3. Confidentiality in the simple secure client
   Rating - **5**

4. AppendFile implementation and efficiency
   Rating - **5**

5. Sharing implementation
   Rating - **4**
   - Inefficient implementation of encryption as each entry in sharing structure is encrypted separately.

6. Revocation implementation
   Rating - **4**

7. Clarity of the design document
   Rating - **4**
   - Fairly clear.

Major Bugs/Flaws:

1. Password is used in file Header in HMAC but is never stored in the User Structure.
2. StoreFile can be called by owner many times. Handling of this scenario is not specified.