Nick Hawkins

CS 610 – Project #4

Design Document

**Summary**

This file server/client program implements additional security features and file sharing capabilities.

Server-side file encryption: All server-side files in each user’s cloud storage will now be stored with the addition of AES encryption. A random 16-character key will be generated for each file being uploaded to the server, and these keys are stored on the client-side of the application to prevent any file on the server from being compromised. These keys will be used to decrypt the files when downloaded back to the client, and all client files will remain unencrypted.

File sharing: Through the client, each user now has the ability to share their cloud storage files with other users with storage in the cloud server. When the user specifies a file and a user to share it with, the encrypted file is copied to that user’s cloud storage.

Synchronization of shared files: In addition, the server remembers the sharing of each file in the system and performs automatic synchronization of those copies in the event the original user modifies or deletes the original file. That same modification or deletion will be passed on to the shared copies given out to other users.

Sharing of AES keys: Also, on the client-side, the user who was given access to the shared file is also given the key to decrypt the file if they choose to download the file. The key will be automatically added to the document of keys the user holds for their respective files in the event a file is shared with them.

Bug fixes: This program now threads the file synchronization process, meaning it will automatically sync when a file in the client has been added, modified, or deleted. Also, the program no longer outputs contents of downloaded files to the console.

**Additional Libraries**

Cipher: The Java Cipher library provided the functionality to encrypt and decrypt blocks of information. In this program, I stored files onto the server after they were encrypted with AES. They are decrypted when downloaded back to the client.