**Cloud storage Encryption/Decryption**

**Description**

Sync Secure Application lets users upload files to Drop box and Google Drive. To secure the files uploaded, the application uses the AES public key encryption algorithm to encrypt the files before uploading. A digital signature is used to digitally sign the files. The files can be decrypted and downloaded only by running the application and providing the correct password entered while uploading the file. The following files can be encrypted: .pdf, .txt, .mp3, .jpg

The application lets the user choose between four options:

1. ***Upload to DropBox:*** Encrypts and uploads the file to DropBox
2. ***Download from DropBox to Local:*** Downloads the file from DropBox to the local machineand decrypts it
3. ***Upload to Google Drive:*** Encrypts and uploads the file to Google Drive
4. ***Sync with Google Drive and Dropbox:*** Encrypts and syncs the file between Google Driveand Dropbox

**Procedure to run the application on an other machine**

1. Download and install the required python packages including the pycrypto module.
2. Download and install the Drop Box and the Google Drive APIs
3. Get the App Key, secret and access token for DropBox
4. Get the Client ID and Secret for Google Drive
5. Create a folder on the local machine
6. Create a .py file in the same folder and copy paste the code (Code At the end of this document)
7. Update the App key, Client ID, access token and Secret in the code.
8. Run the program in IDLE, MAC terminal or in the windows command prompt.
9. When asked for the filename, give the filename of a file which is in the same folder as the .py file.

**REFERENCES**

https://pypi.python.org/pypi/pycrypto https://console.developers.google.com https://www.dropbox.com/developers https://docs.python.org/ http://en.wikipedia.org/wiki/Block\_cipher\_mode\_of\_operation https://www.youtube.com/watch?v=lSrrhP2vFS8

CSE 6331 Cloud Computing Assignment - 1 (Sumanth Pikkili - 1001100941)