

CS 251:SSL Project (Secure Personal Cloud)

3men_in_a_shell

November 23, 2018

Declaration

I acknowledge and understand that plagiarism is wrong. This project is my own work, or my group's own unique group project. I acknowledge that copying someone else's work, or part of it, is wrong, and that submitting identical work to others constitutes a form of plagiarism.

1 Team Details

- Shubham Atri (170050038)
- Debabrata Mandal (170050073)
- Sumit (170050111)

2 Introduction and Motivation

2.1 Project Overview

In this project we have build a primitive cloud storage system. A linux command 'spc' is used to upload and download files(with encryption) from linux client.Using the webclient also, files can be uploaded and downloaded(with encryption).Webclient can also be used to view files.

Encryption schemes used:

- 1.AES
- 2.DES
3. Blowfish

2.2 Why we chose this project

Although all projects were stated to be equally difficult, this project seemed most interesting and challenging than its counterparts.We all use google drive and are fascinated by its functionality and we wanted to get the 'feel' of how google drive works.Moreover, besides web development and databases, encryption(which we knew nothing practically about).Also, we don't like e-games and the progress-tracking app also didn't look interesting.

3 Features

- Signing up using linux client or web client to avail file storage facility
- Upload/Downloaded of files using linux client using 'spc' command which provides various options
- Upload/Download of files using web client by browsing files from local computer
- Three encryption schemes available(in both linux and web clients) for safety of files on the server
- Can delete or share files with other users using webclient.
- Can sync files in local computer with those on the server using linux client
- Can change the encryption scheme of files present on the webclient also

4 Design and Implementation Details

4.1 Database Design

We have created following 4 tables:

1. *auth_users*
keeps record of users and has following columns:
id,password,last_login,is_superuser,username,is_active,date_joined,last_name]
2. *users_book*
keeps record of files owned by a user and has following columns:
book_pk(book number),name(name given while uploading),owner_id,index(name in linuxclient)
3. *users_bookindex*
keeps record of details of a particular book and has following columns:
book_index_p(book number),mimetype(type of file),filename(name in linuxclient),bytes(file converted into binary)
4. *shared_with*
keeps record of users with which a particular file has been shared and has following columns:

4.2 Web Client

We have used django server and made webclient using django. The webclient has file upload and download functionality which has been exploited to upload/download files from linuxclient using 'request' library of python and files can also be uploaded/downloaded using webclient itself. Files can also be deleted and shared with other users.

4.3 Linux Client

Linux Client has 'spc' command to interact with the server using following options:

- help—————- Displays various options available.
- sync—————- Syncs the files on linux client with server
- -version—————- Displays the version of sync
- status—————- Displays files present on server alone, client alone and both client and server
- set-url—————- For signing up
- en-de list—————- Show list of available encryption schemes
- en-de update—————- Update encryption scheme
- en-de dump filepath—————- Update encryption scheme
- en-de upload filepath—————- Update encryption scheme from file present at filepath
- server—————- Displays ip-address and port number of server
- login—————- For logging in
- logout—————- For logging out
- observe—————- Saves a directory to be synced with the server

Note : Files can't be deleted/shared using Linux Client.

4.4 Users

The details pertaining to a user are stored in 'auth-users' table. Care has been taken to prevent user from doing something without logging in. User is allowed to use any of the 2 encryption schemes specified.

The webclient has signup, login functionalities and user is also allowed to change password, upload/download/share/delete files.

4.5 Encryption

Encryption schemes used are:

1. AES (using 'pyAesCrypt' library of python 3)
2. DES (using 'pyDes' library of python 3)
3. blowfish (using 'blowfish' library of python 3)

4.6 Additional/Optional features implemented

1. Deletion and sharing of files using webclient.
2. File upload/download(with encryption/decryption) using webclient.
3. Periodically asking user to sync local files with server.
4. Username and password can be changed.

5 Individual Contributions

- Shubham Atri(170050038)
Made 'spc' command using which files can be uploaded/downloaded to a server.Helped in synchronising encryption done by linux client with encryption done by web client.Also implemented md5sum checking functionality while uploading/downloading files.Helped in making installation scripts.
- Debabrata Mandal(170050073)
Made web client and database using django which has file upload/download functionality.Helped in synchronising encryption done by linux client with encryption done by web client.Helped in making installation scripts.
- Sumit (170050111)
Worked on encryption schemes and helped in synchronising encryption done by linux client with encryption done by web client.Prepared 'man' page for 'spc',project report and user manual.Helped in making installation scripts.
Weightages:
Shubham Atri(170050038) : 37%
Debabrata Mandal(170050073) : 37%
Sumit (170050111) : 26%

References

- [1] <https://simpleisbetterthancomplex.com>
- [2] https://github.com/victor-o-silva/db_file_storage/releases/tag/0.5.2
- [3] <https://stackoverflow.com>
- [4] <https://stackoverflow.com/questions/2435283/using-des-3des-with-python>
- [5] <https://github.com/the-javapocalypse/Python-File-Encryptor/blob/master/script.py>
- [6] <https://stackoverflow.com/questions/3431825/generating-an-md5-checksum-of-a-file>
- [7] <https://stackoverflow.com/questions/2010481/how-do-you-get-all-the-rows-from-a-particular-table-using-beautifulsoup>
- [8] <https://www.linuxjournal.com/content/creating-custom-man-pages>
- [9] <https://askubuntu.com/questions/244809/how-do-i-manually-install-a-man-page>