PROPOSAL

By: - Sanket Barman (2K19/CO/339)
Sanyam Srivastava (2K19/CO/341)

TOPIC: - Secure File Storage on Cloud Using Cryptography

Introduction:

The proposed model is liable to meet the required security needs of data center of cloud. For data security and privacy protection issues, the fundamental challenge of separation of sensitive data and access control is fulfilled. Cryptography technique translates original data into unreadable form. So only authorized person can access data from cloud server.

- The project is based into 2 components one is **backend server API** for the upload and download of **Google cloud storage** and second is the encryption and decryption algorithm **(DES).**

- In this project we will try to implement a Backend server **API for uploading and downloading a file** from the Google cloud storage (Google drive) and **DES (Data Encryption Standard)** algorithm from scratch (without any use of pre-existing libraries).

- The Google cloud storage will be accessed on the authorization by the user by signing in to Google drive and generating access token for the authentication, for the access of Google drive using Google OAuth 2.0.

DES Algorithm:

- The Data Encryption Standard (DES) is a symmetric-key block cipher. DES is an implementation of a Feistel Cipher. It encrypts data in blocks of size of 64 bit each, means 64 bits of plain text goes as the input to DES, which produces 64 bits of cipher text.

- The same algorithm and key are used for encryption and decryption, with minor differences. The key length is 56 bits. DES consists of 16 steps, each of which is called as a round. Each round performs the steps of substitution and transposition.

Backend API and Cloud storage:

- The API will be used to encrypt the file and then upload the encrypted file, download the encrypted file and then decrypt it. The file when uploaded, API will give the file Id and which can be later used to download the file.

- The API will first ask for the access of google cloud storage (using the google drive API) and then the user will be authenticated using Google OAuth 2.0 which will generate an access token and give access to the drive.

Key-Features:

- DES encryption will ensure that the file is secured on the cloud server. The cipher file will be visible to all the people on the server but the cipher file could be decrypted by the authorized user.
- When the authorized user will request the file, the file will be decrypted using the secret key provided and the user will be able to download the file which will be decrypted on the client side.
- This ensures that there is secure file storage and transfer on cloud using encryption. Data is kept secured on cloud server which avoids unauthorized access.
- The following system ensures secure file storage on cloud.

Tools Used:

- ✓ Google Drive API
- ✓ Google OAuth 2.0
- ✓ NodeJS
- ✓ JavaScript
- ✓ Postman

References:

- ✓ https://www.researchgate.net/publication/261281256_Design_and_implementation_of_algorithm_for_DES_cryptanalysis
- ✓ https://www.researchgate.net/publication/325889056_Secure_Cloud_Using_Cryptography