Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

# CSU33032 Advanced Computer Networks Project #2: Securing the Cloud

**Yi Ren, 20304391**

April 19, 2023

## 1 Documentation

For this project, I developed a secure cloud storage application that secures all files that are uploaded to the cloud, such that only people that are part of the "Secure Cloud Storage Group" will be able to decrypt uploaded files. I used python as the programming language for the back-end, and HTML for the front-end. I used Django framework since it gave me everything by default and hence reduced a lot of development time.

### 1.1 Basic Design

For the basic design, I have a page for creating accounts and another page for login. The accounts created will be stored in the Django database and can be checked from the sqlite file generated by Django. When clicked into the homepage, there is a textbox for the user to create a new group. Each group has a public key and a private key when it is generated. The user who created the group will automatically become the manager of the group. At the homepage, the user can see the groups they are in and the groups they are currently managing. Exiting from groups and the group managing are also done at the homepage. A manager of the group has the authority to add users to the group and remove users from the group. Every group member can exit a group on their own side of web page. However, if the manager wants to leave his/her own group, the manager should first transfer the position of manager to another group member, then exit the group.

### 1.2 File Handling

The user can upload file to a certain group at the bottom of the homepage. On the file list page, every group member can see all files uploaded to the group they are in. On the other side, no files in other groups can be seen if the user is not a member of those groups. Every member has the authority to upload files to the group, as well as to delete any files in the group.

### 1.3 Cryptography

For the cryptography, I used RSA and AES to implement a hybrid cryptography. The program will randomly generate an initial vector and choose a random value to use as an AES key, encrypt the file using AES and that key, then encrypt the AES key using the RSA public key of the group that includes the encrypted file. The reason for me to choose a hybrid cryptography solution is that AES, as a symmetric encryption, quickly encrypts large amounts of data, while RSA is encrypts more securely with two keys but in a much slower running speed. Hence, this will be a symmetric encryption algorithm to actually encrypt the file, then an asymmetric encryption algorithm to encrypt the symmetric key to each public key, which combine the strengths of AES and RSA encryption.

## 2 Code

The complete code can be checked from the link below:
https://github.com/YiRen117/Advanced-Computer-Network