Google Cloud-Based Secure File Storage & Sharing System (Enigma)

CLOUD COMPUTING COURSE PROJECT REPORT

Submitted by

Group 17

Amrit Gupta (211000008)

Anirban Bhattacharjee (211000010)

Polisetti Vinay Kiran (211000037)

Under the guidance of

Dr. Kavita Jaiswal
(Assistant Professor, IIITNR)

Dr. Shyama Prasad Mukherjee International Institute of Information Technology, Naya Raipur

1. Abstract

The following project encompasses the ability to hold user data securely with the help of cloud-based storage services.

The Google Cloud-Based Secure File Storage System aims to provide a secure and reliable file storage solution for individuals and organizations using the Google Cloud Platform. The system uses advanced encryption and access control mechanisms to ensure stored files' confidentiality, integrity, and availability. The project incorporates Google Cloud to provide a robust storage and access control solution. The system's key features include data encryption, role-based access control, and data backup. This project aims to provide a scalable and cost-effective solution for secure file storage in the cloud, suitable for a wide range of use cases, including personal, enterprise, and government applications.

2. Introduction

In today's digital age, the need for secure and reliable file storage solutions has become increasingly important. With the rise of cloud-based solutions, many individuals and organizations have turned to cloud storage to store and access their files. One such solution is Google Drive, a cloud-based storage solution provided by Google. Google Drive offers users the ability to store, share and access their files from anywhere, at any time.

However, concerns over the security of data stored in the cloud have led to the development of advanced encryption and access control mechanisms. To this end, this project proposes a Google Cloud-Based Secure File Storage System that leverages the power of the Google Cloud Platform to provide a robust and secure file storage solution.

By utilizing the Google Drive API, provided by the Google Cloud Console, the system aims to provide encrypted file storage and the feature of groups for giving access to the files by managing folders and access to them in the cloud.

3. Background

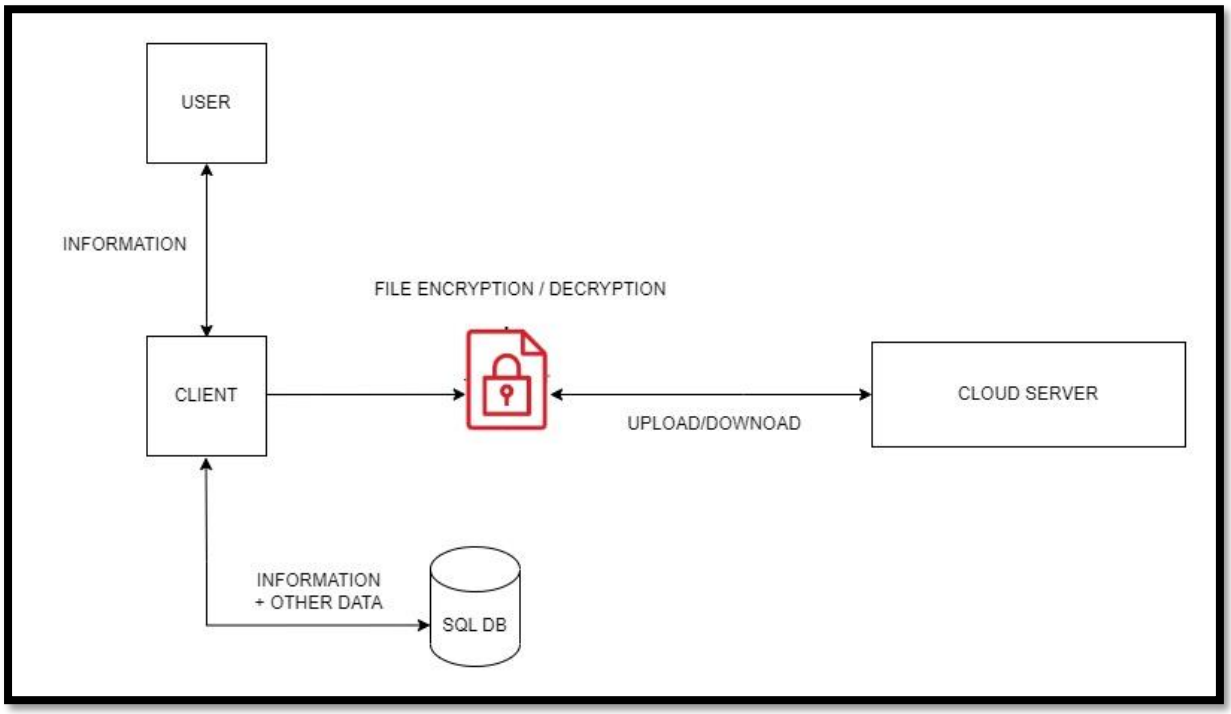
The popularity of cloud storage has increased significantly in recent years, and more and more individuals and businesses are using cloud storage services like Google Drive to store their important data. However, security is a significant concern when it comes to cloud storage as data is stored on servers outside of the user's control. Thus, it is crucial to ensure that the data stored in the cloud is encrypted and secure from any possible data leaks.

Enigma is a secure cloud storage application that aims to address this concern by providing a secure way to store and share files on Google Drive. The application utilizes

a combination of asymmetric and symmetric encryption to secure files stored in the cloud. The user's private key is encrypted with AES and stored with their account, and the group private key is encrypted with the owner's public key.

The application also allows users to create and manage groups, and files can be uploaded and downloaded to the group folder. All files are encrypted when uploaded and decrypted when downloaded, ensuring that data is protected at all times. The application is easy to use, and users can log in with their Google Account, and a folder named SECURE is created in the user's root folder of Google Drive upon login.

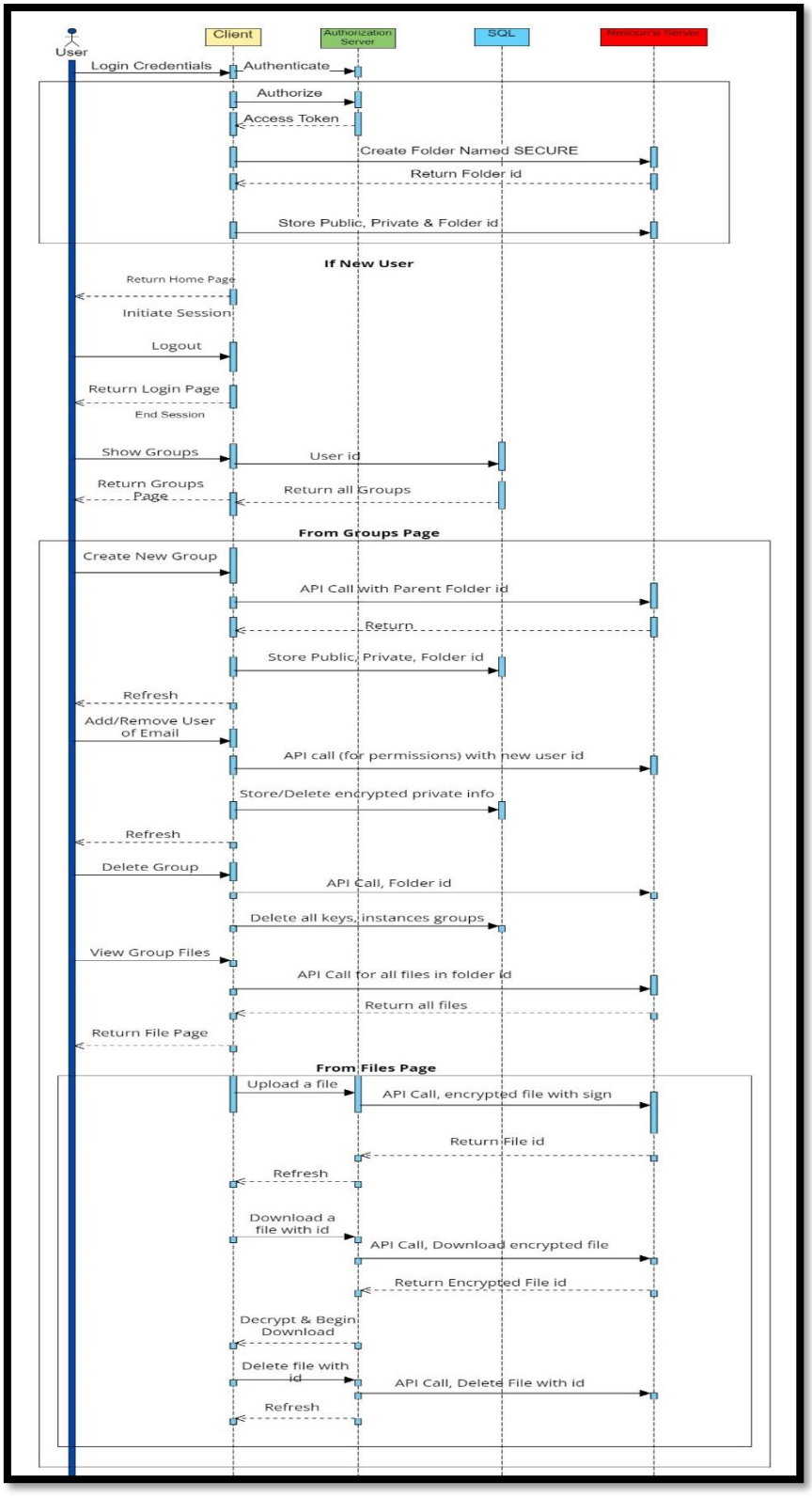
4. Architecture



The user interacts with a website which acts as a client for any API calls made for the user. Prisma ORM is a modern, type-safe database toolkit that simplifies database access and management for application developers. Prisma is used to access the MySQL database associated with the project to get important data that gets stored. The files will get uploaded to the cloud server after encryption and decrypted at the front end which gets returned to the user. The website is written with the help of react.js and next.js. They are equipped with all the necessary features to create the required website with all the functionalities required.

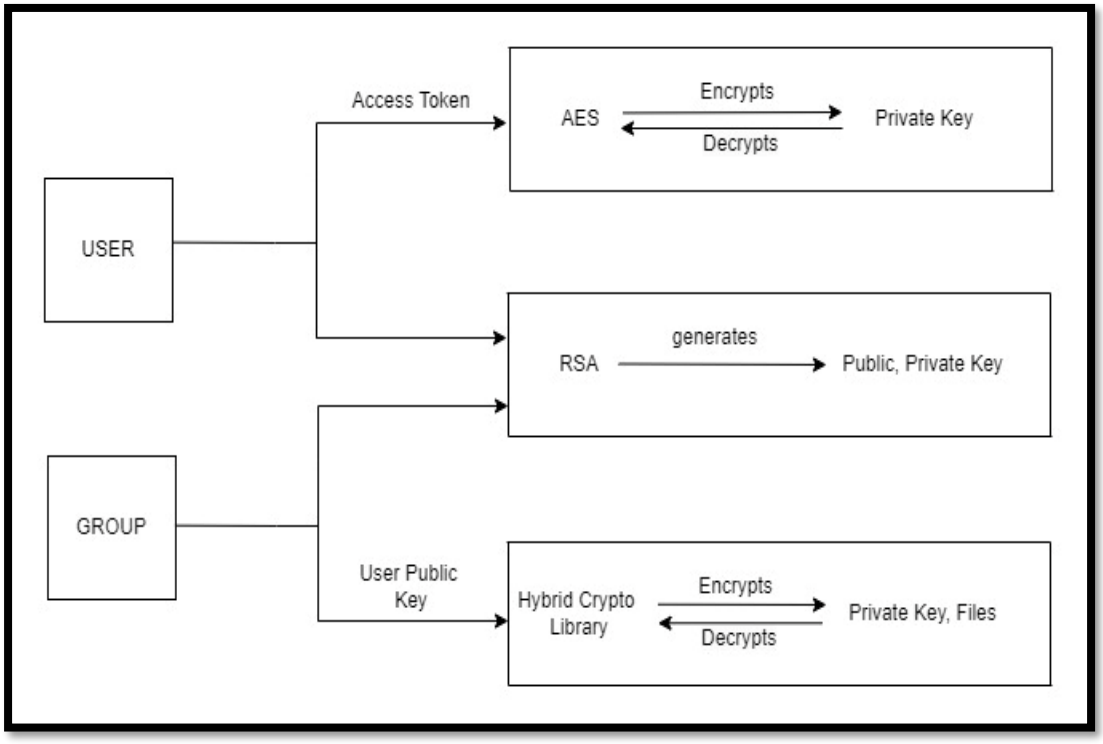
5. System model

A Sequence Diagram below which demonstrates the working of the project in detail and the use, and duties of various entities involved.



View a clear image by [clicking here]

The visual representation of the Cryptography involved with the project is displayed below –



The Technical Description of the Cryptography involved with the project is displayed in the table below –

1. User account created
    i. Public and private Keys are created for the user.
    ii. The user's private key is encrypted with AES with the user's account.
    iii. The public & encrypted private user keys are stored with the user's account.
    iv. The SECURE folder is created on Google Drive and the ID of the folder is stored with the user.
2. Group created
    i. Public and private keys are created for the group.
    ii. The group private key is encrypted with the owner's public key
    iii. The group public key is stored with the group and the encrypted private key is stored with the user and links back to the group.
    iv. The group folder is created in the owner's folder and the group folder ID is stored with the group.
3. User added to a group
    i. The user decrypts their own private key with their session.

ii. The user decrypts the group’s private key with their decrypted private key.
iii. The group private key is encrypted with the public key of the user that is being added.
iv. The group folder is shared with the user through Google Drive

4. User removed from the group

i. The user's connection to the group is removed and their encrypted access to the group’s private key is removed.
ii. The user is unshared from the Google Drive folder.

5. File Uploaded

i. The file is encrypted with the group's public key on the upload.
ii. The file is uploaded to the group folder in Google Drive.

6. File Download

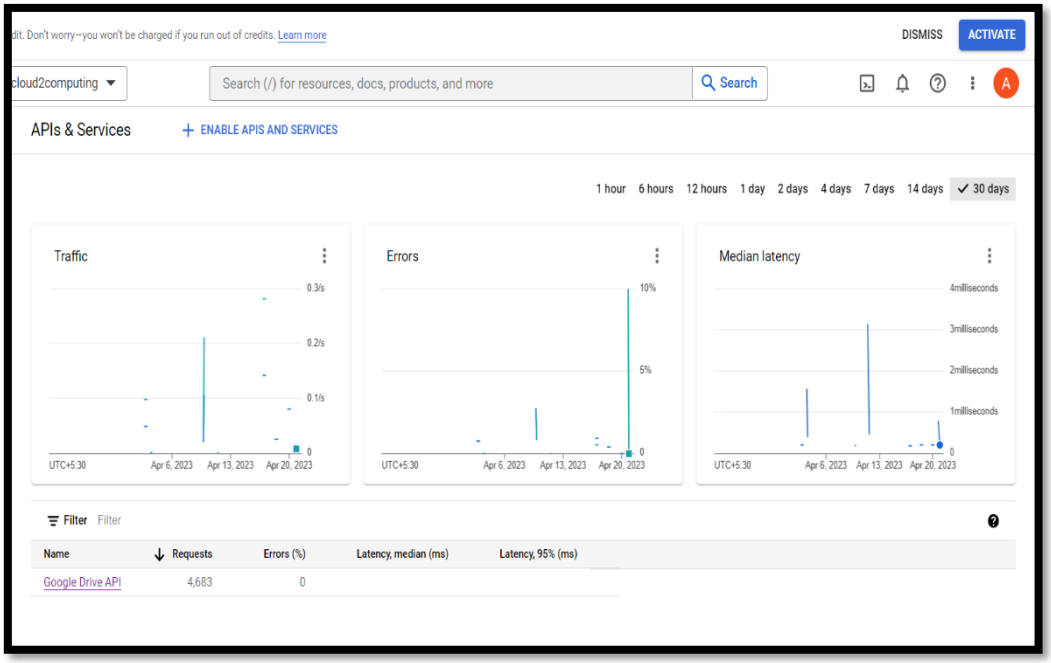
i. The user decrypts their own private key with their session.
ii. The user decrypts the group’s private key with their decrypted private key.
iii. The decrypted group private key is then used to decrypt the file.
iv. Decrypted file is then sent to the user.

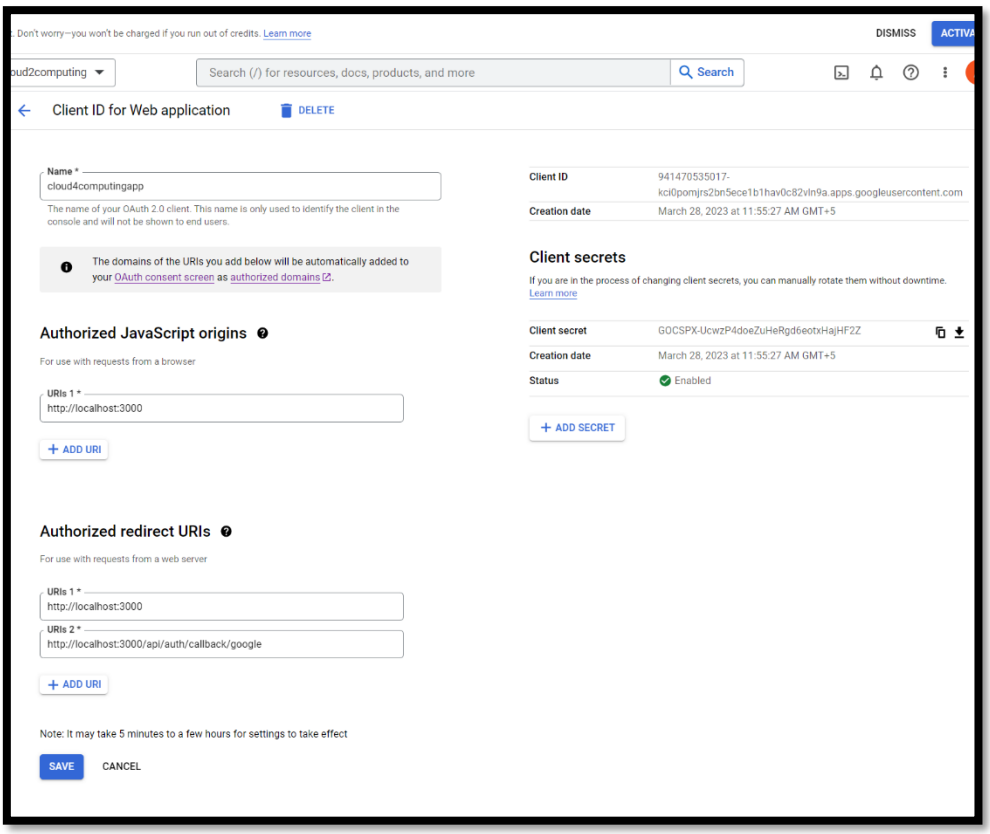
6. Cloud Technology

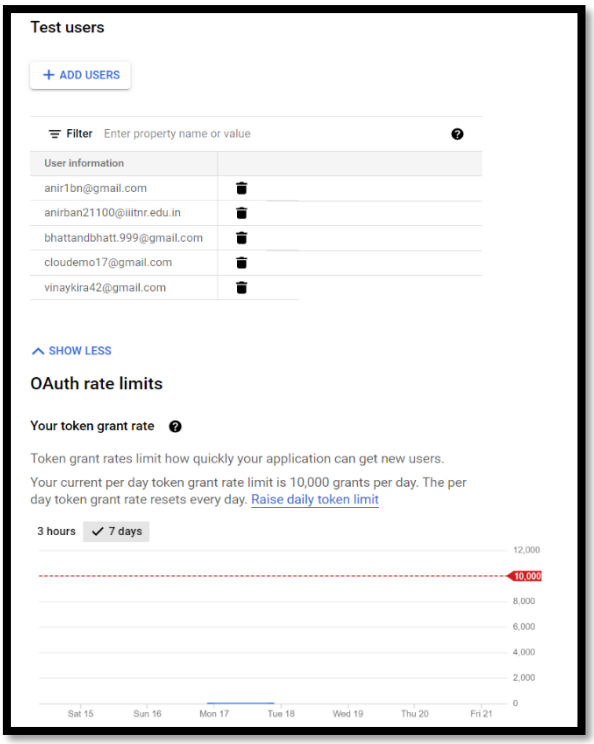
NextAuth is a flexible authentication library for Next.js projects that provides a simple way to add authentication to your application with support for many authentication providers such as Google, Facebook, and more. It also supports email and password authentication, as well as custom authentication providers. NextAuth provides a simple and unified API for working with various authentication providers, and it handles the heavy lifting of authentication flows, such as redirecting users to the provider's login page and handling the OAuth2 authentication flow. Google Cloud Console uses OAuth2.

Google Cloud Console is a web-based platform that allows users to manage their resources and services on the Google Cloud Platform (GCP). It provides an easy-to-use interface for managing and deploying cloud resources such as APIs, monitoring tools, and more. The Google Cloud Console is a key tool for developers, administrators, and businesses looking to leverage the power of cloud computing.

Access tokens are credentials used to access protected resources. In the context of web applications and APIs, an access token is typically a string of characters that grants a client (such as a web application or mobile app) permission to access specific resources on behalf of a user. It will be returned after successful authentication and authorization of the requested scopes from Google. It has to be provided in headers for any API calls.


dit. Don't worry—you won't be charged if you run out of credits. Learn more
DISMISS
ACTIVATE
cloud2computing
Search (/) for resources, docs, products, and more
Search
APIs & Services
ENABLE APIS AND SERVICES
1 hour 6 hours 12 hours 1 day 2 days 4 days 7 days 14 days 30 days
Traffic
0.3/s
0.2/s
0.1/s
0
UTC+5:30 Apr 6, 2023 Apr 13, 2023 Apr 20, 2023
Errors
10%
5%
0
UTC+5:30 Apr 6, 2023 Apr 13, 2023 Apr 20, 2023
Median latency
4milliseconds
3milliseconds
2milliseconds
1milliseconds
0
UTC+5:30 Apr 6, 2023 Apr 13, 2023 Apr 20, 2023
Filter Filter
Name Requests Errors (%) Latency, median (ms) Latency, 95% (ms)
Google Drive API 4,683 0


Don't worry—you won't be charged if you run out of credits. Learn more
DISMISS
ACTIVA
oud2computing
Search (/) for resources, docs, products, and more
Search
Client ID for Web application
DELETE
Name *
cloud4computingapp
The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.
The domains of the URIs you add below will be automatically added to your OAuth consent screen as authorized domains.
Authorized JavaScript origins
For use with requests from a browser
URIs 1 *
http://localhost:3000
ADD URI
Authorized redirect URIs
For use with requests from a web server
URIs 1 *
http://localhost:3000
URIs 2 *
http://localhost:3000/api/auth/callback/google
ADD URI
Note: It may take 5 minutes to a few hours for settings to take effect
SAVE
CANCEL
Client ID
941470535017-kci0pomjrs2bn5ece1b1hav0c82vln9a.apps.googleusercontent.com
Creation date
March 28, 2023 at 11:55:27 AM GMT+5
Client secrets
If you are in the process of changing client secrets, you can manually rotate them without downtime.
Learn more
Client secret
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
Creation date
March 28, 2023 at 11:55:27 AM GMT+5
Status
Enabled
ADD SECRET



Benefits of using Google Cloud for this project –

1. Accessibility: One of the biggest advantages of the cloud is that it allows users to access their files and data from anywhere and on any device with an internet connection. This means that users can easily share files and collaborate with others, even if they are in different locations.
2. Scalability: Cloud storage solutions allow users to easily scale their storage needs up or down as their needs change. This means that users can easily add or remove storage capacity as needed, without having to worry about the costs and logistical challenges of managing physical storage devices.
3. Cost savings: Using cloud storage can be more cost-effective than maintaining physical storage devices. With cloud storage, users pay only for the storage capacity they need, rather than having to purchase and maintain expensive hardware.
4. Collaboration: Cloud storage solutions often include collaboration features that make it easy for users to share files and data with others, collaborate on documents in real-time, and manage shared projects.
5. Maintenance: Cloud storage providers typically handle maintenance and updates for the underlying infrastructure, which means that users don't have to worry about managing and maintaining physical storage devices themselves.

7. Result/Conclusions

The project intends to demonstrate how to generate public-private key pairs using RSA, encrypt using AES and Hybrid cryptography, and decrypt the same to provide security within the cloud from data leaks and unauthorized accesses. Encrypting files on the cloud storage this way can help protect important user data. It also shows how files stored on the cloud can be securely shared among only the intended users of the file.

Some screenshots of the final website demonstration are below –

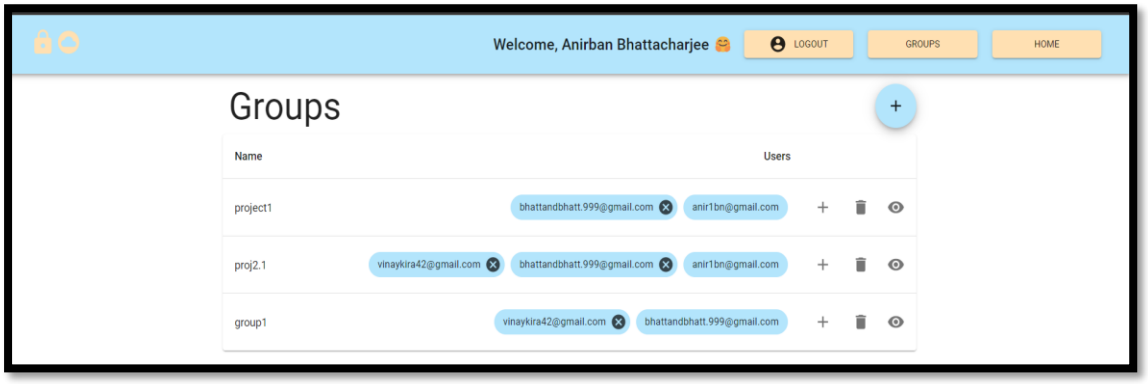


Fig. shows the groups associated with a certain user

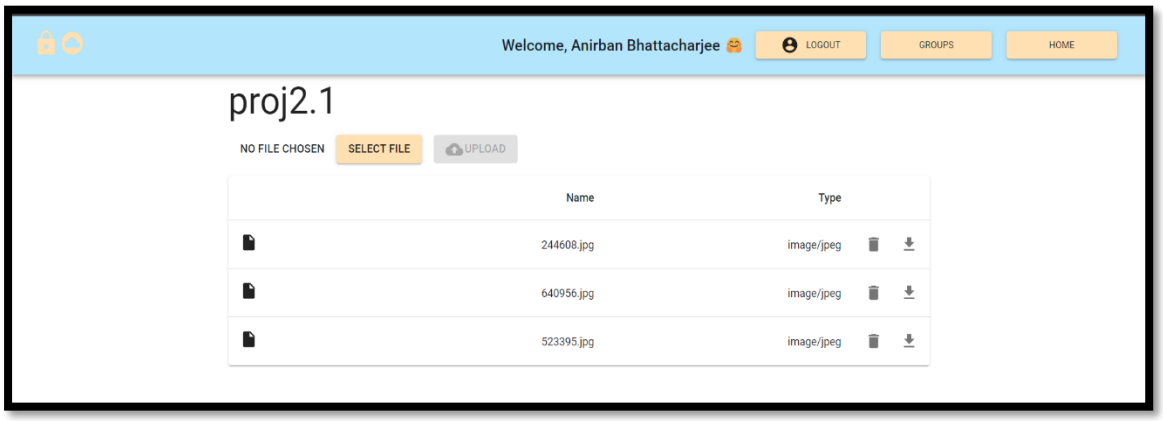


Fig. shows the list of files in a group

Fig. shows the encrypted file from drive of a .txt file