COLLEGE OF NATURAL SCIENCES, MATHEMATICS AND ENGINEERING
CSU BAKERSFIELD

File Storage System Using Facial Pattern Recognition

Jacob Acosta, Carlos Sandoval, John Pocasangre, Andrew Attia Ibrahim

Advised by Dr. Chengwei Lei

Project Summary

Our goal is to make the process of storing files online simple. We aim to achieve this by incorporating facial recognition and Google into a user friendly interface that ensures the user's data is safely stored.

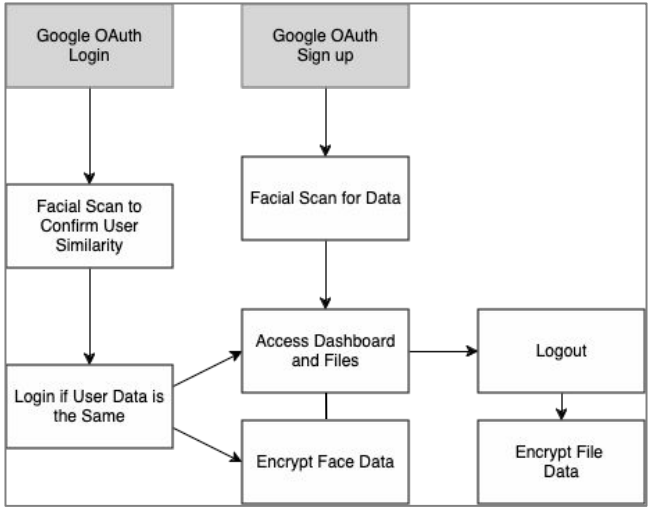
How data is secured

We encrypt our user's files using the AES128-GCM algorithm and making an encryption key with data collected from the Google authentication service (OAuth2). This key then encrypts our user's face data, ensuring that it cannot be tampered with.

Ease of Use

We allow the seamless integration of Google OAuth and the user's face to sign in. In simple terms, if the user already went through the Google OAuth process, all they need to do is use their face to sign in and access our application.

How it works



The facial data consists of 128 different points collected from the person's face. That face data is then encrypted using the AES128-GCM encryption key that is generated using the user's unique Google OAuth data. The user will be allowed to log in successfully if the face data that was encrypted matches at the time of facial rescanning.

Technology Used

File Management

Users can choose to upload files individually, create and upload their files into their newly created folder, or to upload an already existing folder. The user can also chose to rename these files and folders, filter through their entire home directory to find files without going into each of their folders using the search bar, or filter for specific file types. They can also see small previews for their files, and they can download them if they wish to store them locally.

Get Started!

Visit facialrec.org to start storing your files today