Project: Secure Vault

About the Project:

Secure Vault is a mobile application designed to securely store a wide range of sensitive information, including passwords for various platforms, ID/passport card numbers, and bank account details. It offers a convenient and centralized location for managing this critical data while prioritizing user privacy and security.

I)Problems and Solution Objectives:

- **Problem:** Remembering numerous passwords and managing sensitive information across various platforms can take time and effort. Users often resort to weak passwords or storing information in unsecured locations like notes apps or text files.
- **Solution:** Develop a user-friendly mobile app that provides a secure and convenient solution for storing and accessing passwords and sensitive information. It eliminates the need to remember numerous passwords and offers features like:
    - Secure storage with robust encryption.
    - Password generation for creating strong, unique passwords.
    - Easy access to stored information through facial recognition authentication (or a master password).
    - Optional seed phrase recovery for added security.

II) User Characteristics:

Team Members: Achref Khairi Wael Haji

Security-Conscious Users: Users who prioritize the security of their sensitive information and seek reliable solutions for password and data management.

Tech-Savvy Individuals: Users familiar with mobile apps and comfortable using facial recognition technology for authentication.

Busy Professionals: Users who manage multiple accounts and need a convenient solution for storing and accessing passwords and personal information on the go.

III)Features:

1. Password Storage:

- **Theoretical Review:** Passwords are securely encrypted and stored within the app's database using cryptographic algorithms. Access to stored passwords is protected by the user's facial biometrics.
- **Product Review:** Users can securely store passwords for various platforms, such as social media accounts, email accounts, and online banking. They can easily add, view, edit, and delete passwords within the app's interface.

2. Sensitive Information Storage:

- **Theoretical Review:** Other sensitive information, such as identification documents (e.g., ID card, passport) and financial details (e.g., bank account numbers), are encrypted and stored securely within the app.

- **Product Review**: Users can store sensitive information securely, ensuring that their data remains protected from unauthorized access. They can organize and manage their stored information effectively within the app.

3. Facial Recognition Authentication :

- **Theoretical Review:** Facial recognition technology verifies a user's identity based on unique facial features captured by the device's camera. It analyzes facial biometrics to authenticate users securely.
- **Product Review:** From a user perspective, facial recognition simplifies the login process by eliminating the need to remember passwords. Users simply need to scan their faces to gain access to the app, enhancing security and convenience.

4. Master Password Authentication (Alternative):

- **Theoretical Review:** For users who may not have facial recognition available or prefer a traditional method, Secure Vault offers master password authentication. This password should be strong and unique to Secure Vault. We will surely have Gmail linking alternatives.
- **Product Review:** Users can set a master password during signup and use it to access the app. Secure Vault securely stores the encrypted master password.

5. Seed Phrase Recovery :

- **Theoretical Review:** Consider implementing a seed phrase recovery system as an additional security layer. This allows users to regain access to their data on a new device even if they lose their phone or forget their facial recognition/master password. The seed phrase utilizes a standard like BIP39 for compatibility and security.
- **Product Review:** Secure Vault can generate a unique 12-word seed phrase during signup. Users are prompted to write down the phrase and store it securely offline (e.g., on paper in a safe location). If needed, they can use the seed phrase to recover their data on a new device.

6. Password Strength Analyzer:

- **Theoretical Review**: Users can assess the strength of their passwords and receive recommendations for improvement.
- **Product Review:** Users input their passwords into the app's strength analyzer tool, which evaluates factors such as length, complexity, and uniqueness. The tool provides feedback and suggestions for creating stronger passwords, such as increasing length or adding special characters.

IV) Functional Flow:

1. **User Registration and Facial Recognition Enrollment:**
    - Users download and install the app from the app store.
    - Upon the first launch, users register for an account by providing basic information and setting up facial recognition authentication.

- Users enroll their facial biometrics by capturing multiple facial images for future authentication.

2. **Login and Access:**
    - Users log in to the app using their registered credentials or facial biometrics.
    - Facial recognition technology verifies the user's identity, granting access to the app's features.
3. **Password and Sensitive Information Management:**
    - Users can add, view, edit, and delete passwords for different platforms within the app.
    - Similarly, users can store and manage other sensitive information, such as identification documents and financial details, securely.
4. **Facial Recognition Authentication:**
    - Each time users access the app or sensitive information within the app, they authenticate themselves using facial recognition.
    - The app captures and analyzes the user's facial biometrics to verify their identity and grant access securely.
5. ***Password Strength Analyzer:***
    - Users input a password into the app's strength analyzer tool.
    - The tool evaluates the password's strength based on predefined criteria such as length, complexity, and uniqueness.

- Users receive feedback and recommendations for improving the password's strength, such as adding special characters or increasing length.

6. **Encryption and Data Security:**
    - Passwords and sensitive information stored within the app are encrypted using strong cryptographic algorithms.
    - Access to stored data is protected by the user's facial biometrics, enhancing security and preventing unauthorized access.
7. **User Interface and Experience:**
    - The app features an intuitive and user-friendly interface, allowing users to navigate and interact with ease.
    - Visual cues and feedback guide users through the authentication process and data management tasks, enhancing the overall user experience.

V)General Constraints:

Device Compatibility: The app must be compatible with a wide range of mobile devices, including smartphones and tablets, running on popular operating systems such as iOS and Android.

Network Connectivity: While basic features may function offline, certain functionalities, such as data synchronization and updates, require internet connectivity.

Storage Capacity: The app's storage capacity may be limited by the user's device storage, impacting the amount of data that can be stored locally.

VI) Assumptions and dependencies:

Facial Recognition Accuracy: The facial recognition technology employed by the app is assumed to be accurate and reliable, ensuring seamless authentication for users.

Data Encryption and Security: It is assumed that the app employs robust encryption techniques to secure stored passwords and sensitive information, protecting them from unauthorized access.

User Cooperation: Users are assumed to follow recommended security practices, such as keeping their device and app updated, setting strong passwords, and safeguarding their facial recognition enrollment data.

User interface: The system should provide a user-friendly interface that allows users to interact with the system easily

Performance: The system should be able to work on its functions quickly and efficiently, but also handle a large amount amount of data without crushing down.

Security: The security in our app is a top-tier importance. The system should ensure that stored data isn't available for anyone and that it's encryption is very sophisticated.