DBMS Project

**Topic:**Password Manager

Implementation of Password Manager using HTML, CSS and JS for frontend and PHP and SQL for backend.

**Group Members:**

1. Mahendra Anit Sinai Priolkar
2. P Jeevesh Naidu

**Motivation:**

Password managers are vital tools that can help you stay safe online and be more digitally secure by simplifying the process of using strong passwords. It is quite sad that some people are very advanced in technology and knowledgeable in the latest trends but do not care about protecting their accounts, many of which are linked to their personal identity.

Maintaining and remembering so many passwords in today’s world can be difficult. Inorder to manage all of them, Password manager can be a platform where we can store all passwords and just remember one password called as the Master Password which can be used to access all our passwords.

The Password Manager project aims to develop a comprehensive password manager application that addresses the growing need for efficient and secure password management in today's digital landscape. With a focus on security, user-friendliness, and convenience, Password Manager will provide individuals and businesses with a secure platform to store, generate, and manage their passwords and sensitive information.

**Modules:**

1. Authentication Module:

An authentication module is the module that collects user information such as User ID and Master Password, dual verifies with 2FA OTP and compares the information against the entries in the database. This module also has an option to reset password via mail if forgotten.

1. Encryption/Decryption Module:

The Encryption module allows the secure storage of personal data of the users such as Email-ID, Passwords, etc. This module allows an individual’s details to be stored in an encrypted manner. This means that the data is stored in the database in the form such that no individual can read and access it.

Decryption module allows the decryption of the encrypted data so that the user can access and view it in readable format.

1. Password Maintenance Module:

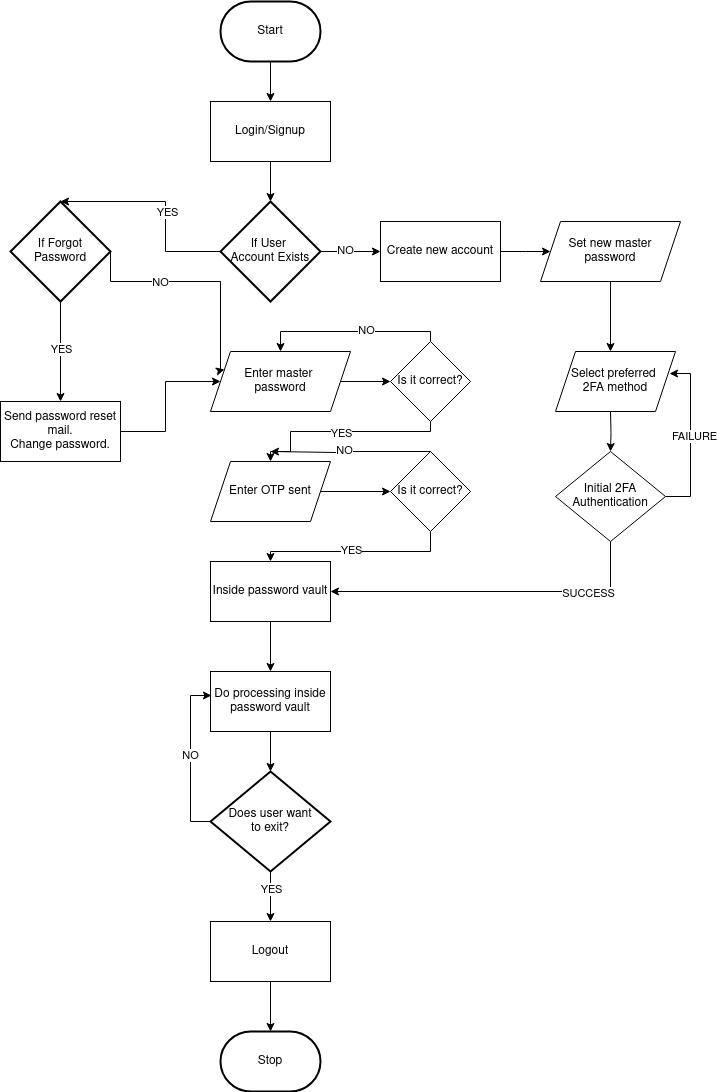
To ensure best practices, account passwords should be updated after some time. If a password can be cracked in N days, it should be changed every N days or better less. This module allows us to set a timely reminder or even specify a script to change the password at a given date. Also, the password manager stores 5 recent passwords in history. If the new password entered by the user matches with any one of them, the user will be prompted to re-enter and thus prevent reuse of passwords.

1. Password Strength Analysis Module:

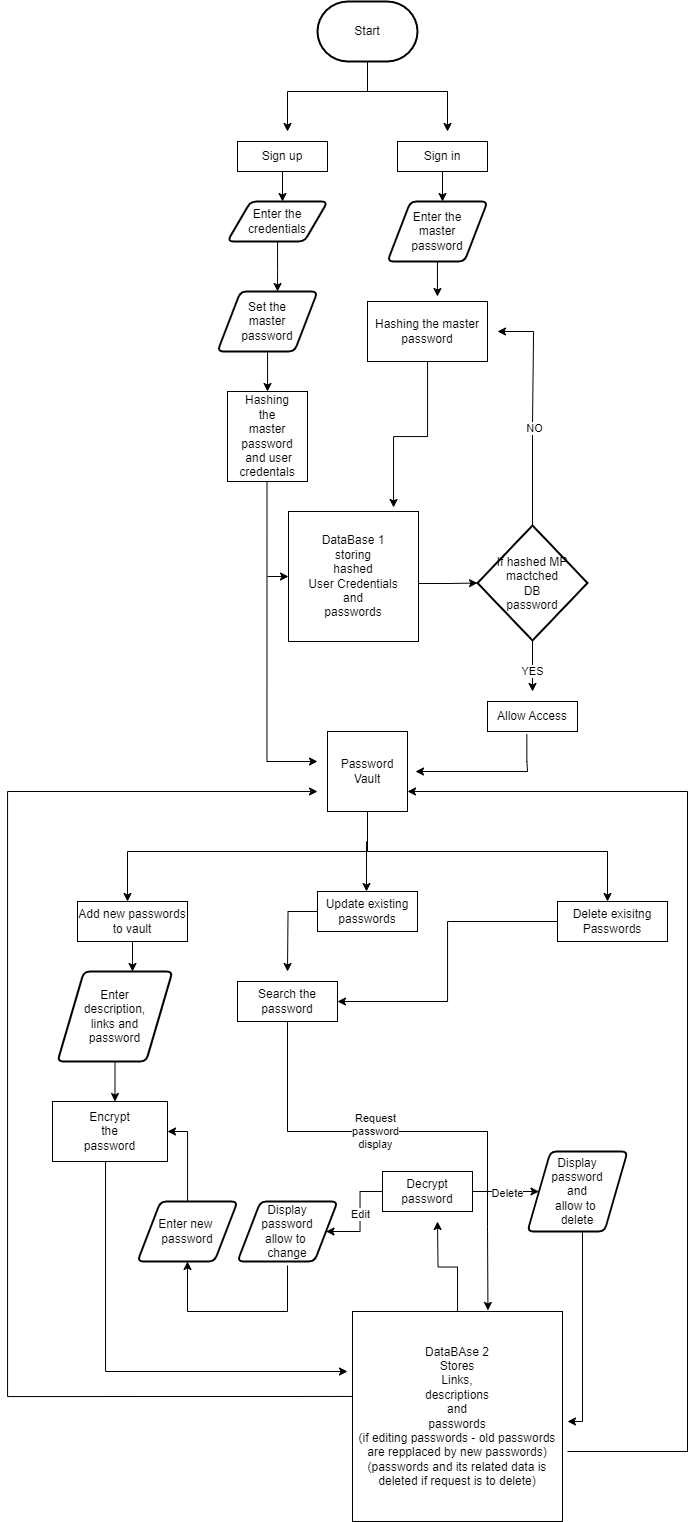
This module gauges the overall strength of a user’s password. If a password was detected in a public data breach, it is extremely unsafe and the user is prompted to change immediately. Also only if the password length > 16 characters and password entropy > 60 bits, the password is deemed secure.

**Flowcharts:**

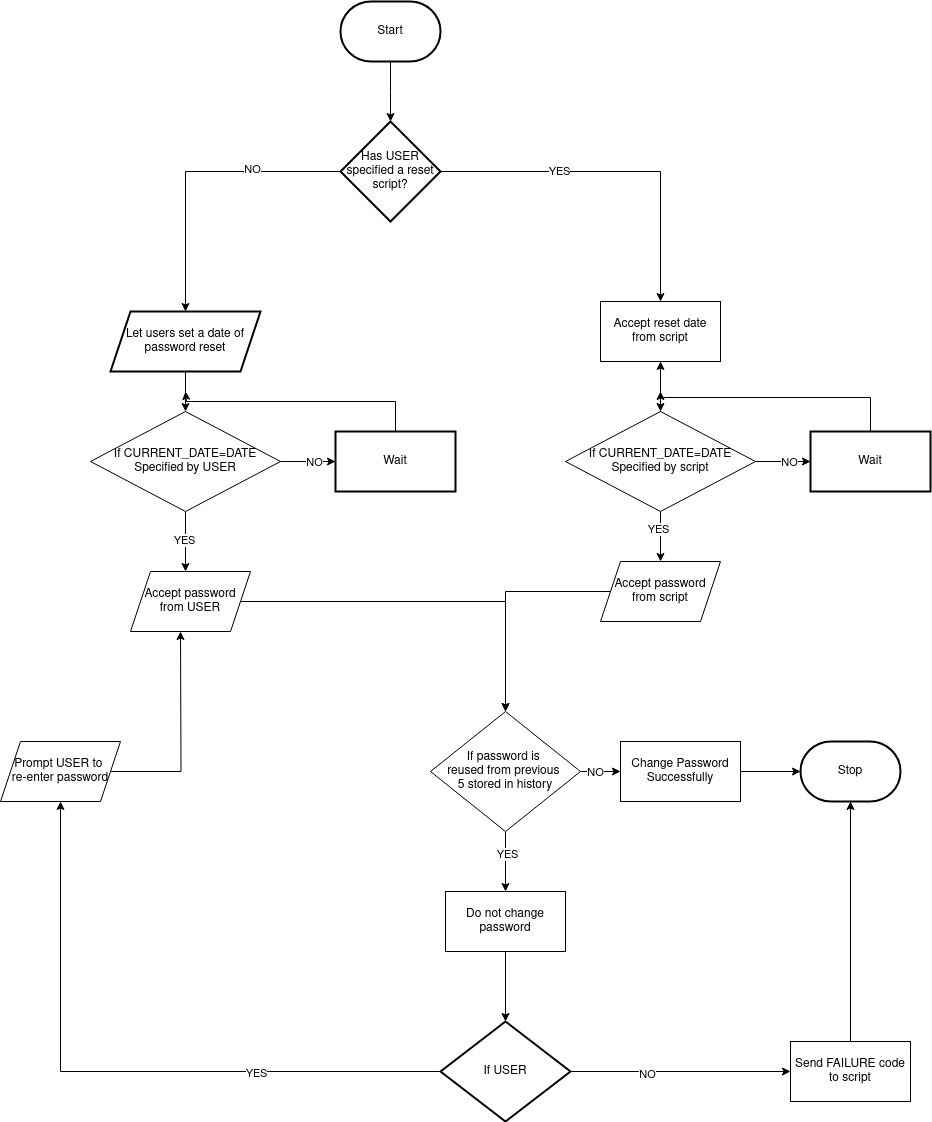
1)Authentication Module:



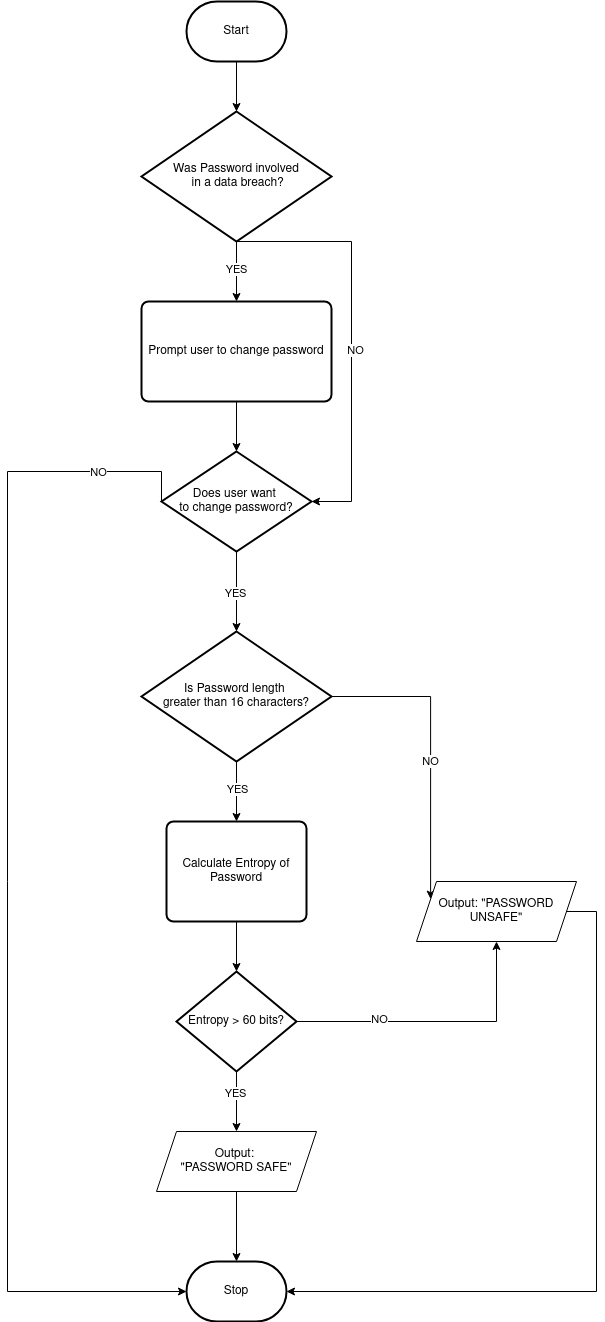
2)Encryption/Decryption Module:



3)Password Maintenance Module:



4)Password Strength Analysis Module:



**Goals:**

1. Online Security
2. Better User Experience
3. Password Management
4. Emergency Credential Access and Recovery

**Application in Real world:**

1. Personal or Business and Professional Uses.
2. Healthcare and Medical Professionals.
3. Developer and IT use.

**Conclusion:**

Password manager will be implemented using HTML, CSS, JS, PHP and MySQL.