**ANGELES UNIVERSITY FOUNDATION**

**College of Computer Studies**

**FINAL PROJECT**

**Password Manager**

**(SEN10)**

**Submitted by:**

David, Pacito Robert Ian

Guevarra, John Lenard

Mendoza, Achim Jonah

Nastor, Ericksson

**Submitted to:**

DR. ROSANNA A. ESQUIVEL

**Introduction**

Password managers are applications that store your passwords in a safe place. The passwords are encrypted when you use this software, and you only need one master password to access them. These passwords are stored on your local computer. To access the database of other passwords for numerous sites and apps, you just need to remember one password. A password manager tool can also offer a variety of other useful features. They frequently have password generators on hand that can be used to generate secure passwords. There are some major concerns to make while utilizing password manager software. Because our password manager saves information on the local computer, you may lose all of your passwords if the computer is reformatted. In order to stay safe online, you must create strong passwords. Unfortunately, complex passwords are difficult to remember; also, each account requires a unique password. If you have ten login passwords for several Internet accounts, for example, remembering them becomes challenging, especially if you change them every three months. Fortunately, like with so many other issues, there is a solution. Password manager organizes your passwords by local program. For each account, you can create complicated passwords that are easy to remember. A password manager is essentially a secure digital vault that stores password login information for apps and accounts on your mobile device, websites, and other services. In addition to safeguarding your identity, credentials, and sensitive data, the password manager includes a password generator to help you establish strong, unique passwords and avoid repeating passwords. With all of the recent news about security breaches and identity theft, having a unique password for can go a long way toward guaranteeing that your password couldn't be used on other sites if one site is compromised. You're basically creating your own security features by utilizing several passwords.

**Background of the Study**

Forgetting a password for a website or software you use to sign in to might lead you down the rabbit hole of trying to figure out how to reset it. It's highly tempting to use a password that is so basic that you won't forget it, or to memorize only one complicated password and use it everywhere. Both techniques, however, are doomed to fail. A hacker, for example, can quickly guess or brute-force a trivial password. A data breach can also disclose whatever complicated password you establish, putting all of your accounts at risk. The only way to avoid this is to use a separate password for each account, one that is both long and random. You won't be able to remember lots of secure passwords. That is why a password manager is essential. If you're constantly getting locked out of online accounts because you can't remember your passwords, it's time to invest in a password manager, which will help you keep track of and manage all of your login credentials while ensuring password security. The goal of this password manager is to keep track of passwords for various online accounts. This application will allow the user to save all of the username and password information for the accounts he has on the internet. These details will be encrypted and preserved in the database. This will assist the user in remembering several usernames and passwords for online accounts. The system should allow the user to create, edit, and remove accounts. To utilize this tool, the user must first log into the system. To get into the password manager, you'll need the master password. All account information, such as the platform, username, and password, will be presented on the screen using our password manager.

**Methodology**

The team used the waterfall approach for this software development. The requirements are gathered and analyzed by the team. Requirements are documented during this phase and clarifications can be sought. Following the completion of the planning phase, an analysis is carried out to determine the suitable business logic, database models, and other elements that will be necessary at this point in the project. Up to this point, all planning, specification, and design documents have been coded and incorporated into the project's first iteration. After this build iteration has been coded and implemented, the next step is to run through a series of tests to discover and locate any potential flaws or issues that have arisen. After all of the previous steps have been finished, it's time to assess the development to this point. This allows the entire team, as well as clients or other external parties, to assess where the project is, where it needs to go, what can or should change, and so on.

**Functionalities**

**Master Password**

* The entire application is protected by a single master password, so you don't have to remember many passwords for different accounts; just remember one and we'll handle the rest.

**Password Generator**

* A password generator is a program that produces a password with a mix of upper and lowercase letters, numbers, and symbols that is strong enough to provide high protection.

**Copy Password and Username**

* Passwords and usernames that are too long or difficult to type? We'll copy the password and user to your clipboard if you tap the Copy Password and Copy User button.

**Update, Remove and Add new data**

* Password manager allows you to add multiple data and update password and username. You also have the capability to remove existing data if you no longer need them.

**Software Development Models**

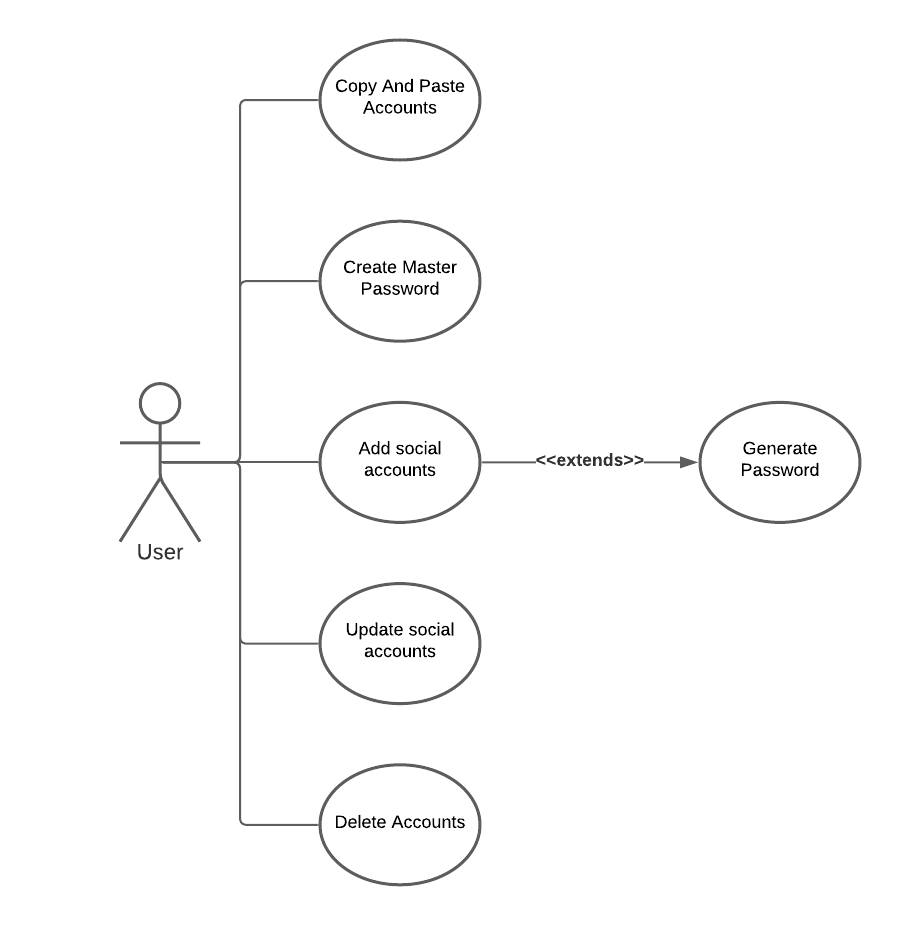


Figure 1: Use Case Diagram

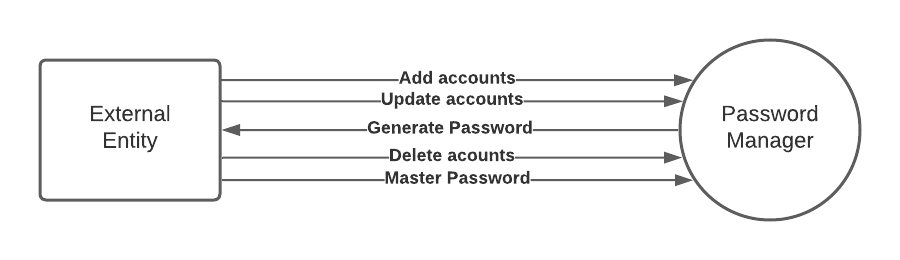


Figure 2: Context Diagram

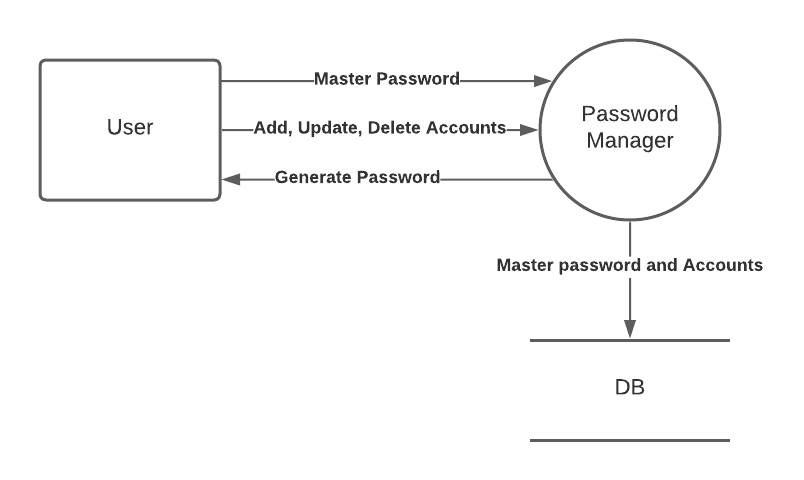


Figure 3: Data Flow Diagram

**User Stories**

As a user, I’d want to have my own password and account manager

As a user, I want to create my own master password

As a user, I’d want to be able to generate a password

As a user, I should have an option to store accounts as many as I like

As a user, I want to have an option to update and delete account

**Screenshot Of the Program**

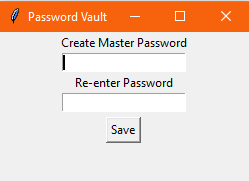


Figure 4: Master Password Creation

This is what the program will look like once we start the program and will ask to create your master password

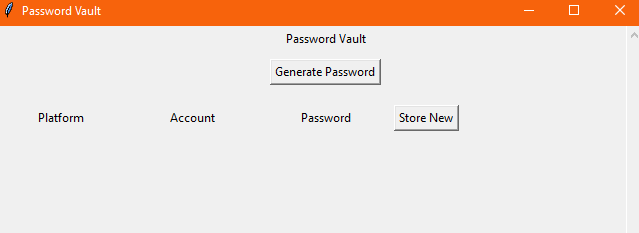


Figure 5: Password Vault Window

After creating your master password, you will now have access to your password vault where you can store new account and generate a password.

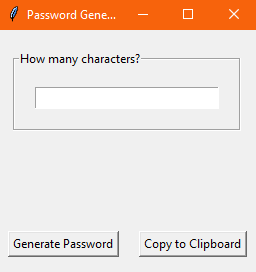


Figure 6: Password Generator Window

When you clicked on “Generate Password” this window will pop up and ask you to enter how many characters you want to have your password. Once the password has been generated, you can click copy to clipboard to easily copy the password.

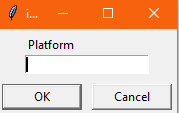


Figure 6: Platform Window

This window is when you click on “Store New” and you will have the option to enter which platform the account is going to be used for (example: Google, Microsoft).

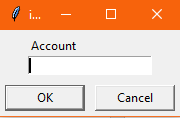


Figure 7: Account Window

After entering the Platform, you will then have the option to enter the account for that platform. (Example email, username).



Figure 8: Password Window

Once done entering your email or username. You can also store your password to your vault.

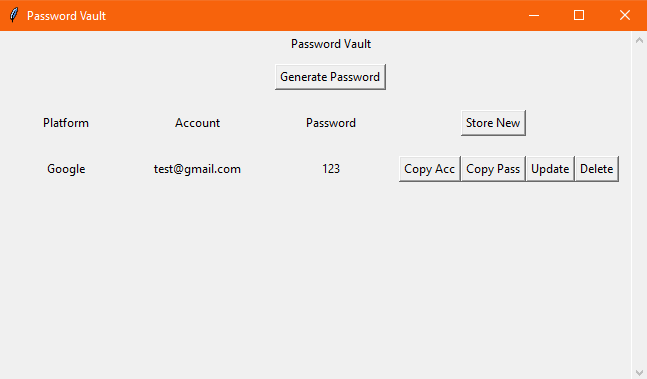


Figure 9: Updated Password Vault

Once done storing all the information, you will see the details on your password vault window where the platform, account and password shows up. You will have the option to copy an account, copy password, update or delete your information.