GE-103
Password Keeper

Ayush Agarwal[#1], Harshit[*2], Priyansh Kashyap[#3],Devangita Sharma[#4]

[1]2021MEB1274, IIT Ropar, India, 2021meb1274@iitrpr.ac.in

[2]2021EEB1175, IIT Ropar, India, 2021eeb1175@iitrpr.ac.in

[3]2021EEB1196,IIT Ropar, India, 2021eeb1196@iitrpr.ac.in

[4]2021EEB1163, IIT Ropar, India, 2021eeb1163@iitrpr.ac.in

***Abstract*— This paper describes how a password management system can store, create and encrypt multiple passwords at a time.**

***Keywords*— Password Generator, Password Manager, Password, Password Security, Password Strength**

I. Introduction

In recent years it has been a noticeable rise in awareness around the world regarding the subjects of password and password security. This has led to a scenario where an individual is supposed to remember a never ending number of hard to remember passcodes. To counter this several password management softwares have flooded the market that help an user by allowing him to remember one password and provide him with access to his wide array of passwords.

II. Literature Review

Similar papers on the discipline talk about the importance of awareness about cyber security, encryption, and emphasize the importance of strong password. They rise in cyber threats being the primary reason for the following. And as the threat of cyber rises we will need stronger passwords and effectively stronger password management services. There have also been discussions on the use of a more modern day solution to this by the coinage of 'passphrase'.

III. Objective

For anyone to survive in this modern world they have to pass through multiple websites and apps and are supposed to remember multiple passwords. The objective here is to remove anyone of this stress.This has been achieved by

a.*Strong Password Generator*- We have created an algorithm which generates the strong password and provides it to the users.

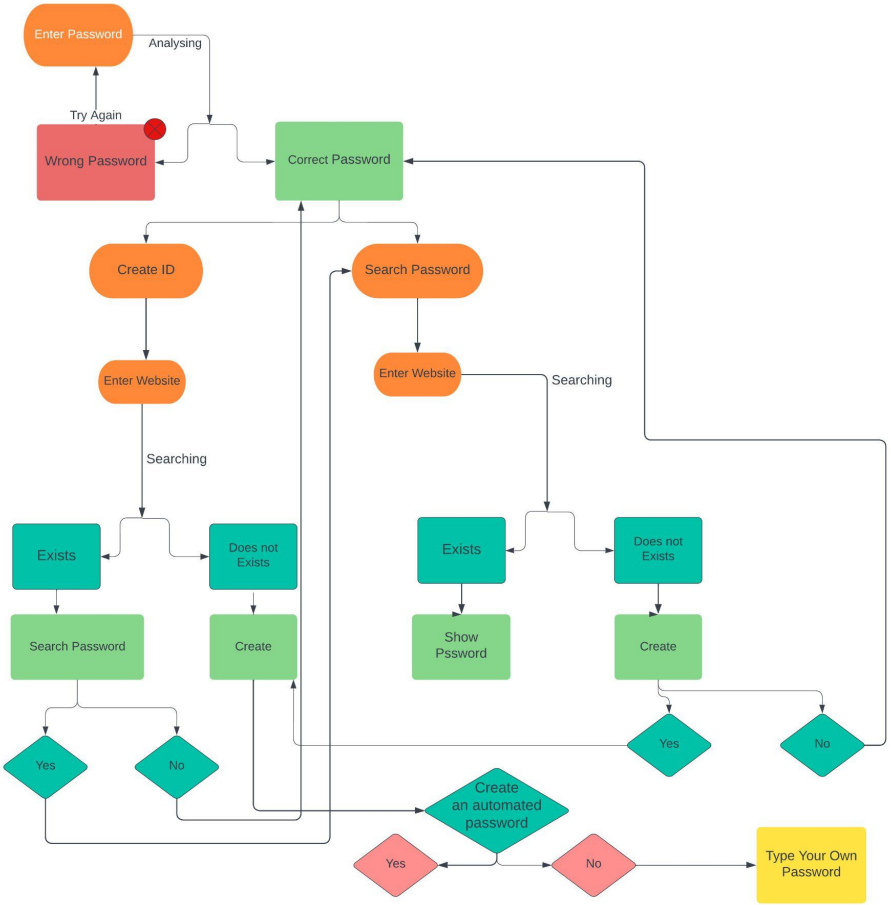
1. Passwords must contain at least one symbol, character(uppercase or lowercase), and a number.
2. It must be of reasonable length so that users can neither forget about it nor be hacked by anyone.

b.Password Creator - The password input by the users or that we provide them, is stored in the secure text file. The text file stores all the passwords of the particular websites input by the users. In particular, if a user mistakenly wants to add a website that already exists in the file then we provide them with an option in which the user can see their password for the already existing website. It then provides them with the choice to either use an automated generated strong password or enter the password manually.

c.Password Finder - It's a search function that finds the already existing websites that the user wants to know the password of the algorithm then provides the user with the password for that particular website..
If a user mistakenly searches for a website that does not exist, we provide them an option to add that website. Along with that they can also add their input password or the password generated by the password generator.

d.Password Security - We have created a default password that every user must input before adding or searching the website. Only three attempts are allowed for the user, and if it exceeds then the user is not allowed to search for the website or to add it.

How the algorithm works is illustrated below with the help of the flowchart.



IV. Conclusions

The algorithm successfully stores, creates, and changes the passwords i.e was a password manager. Further work upon it could lead to development of an effective software manager.

Acknowledgment

We would like to acknowledge Dr. Sudarshan Iyengar for his mentorship and support throughout. We would also like to thank our instructor Ms. Monisha Singh for allowing us to research on such a stupendous topic. We also extend a hand of thanks to our competitive peer group for a healthy learning environment.