**Password Manager and Password Generator**

Abha Marathe,Omkar Karpe

Department Of Computer Science and Engineering

Vishwakarma Institute of Technology Pune, India

***Abstract* —***Everyone who uses a variety of Internet services is concerned with the security and confidentiality of information about attackers. Many authentication systems are available to protect personal data, and the password authentication system is one of them. With increasing information sharing, the popularity of the internet, electronic transactions, and data transfer, both password security and authenticity have become an important and necessary topic. But it is also mandatory to confirm the strength of the password. For the same reason, all the technical experts recommend complex password patterns. But most of the time, users forget their passwords because of those intricate patterns. In this paper, I am proposing a new algorithm which will generate a strong random password, unlike other random password generators available. This password generator creates a password by asking the user if they want lowercase or uppercase letters, special characters, numbers in their password. He can later copy the password to the clipboard. Then we come to the password manager where it asks for a password to access the password manager. When we log in to the password manager, we need to fill in the entry of the website, we want to keep its password, the username required for the website, and then we need to paste the password we copied from the password. generator, or we can enter our own password. Later whenever we need a password, we just need to enter a password and we can access any password we want ...!*

***Keywords*** *— Password manager, Username, Authentication, Password generator.*

# I. INTRODUCTION

Internet security is recently becoming a significant issue with the increasingly wide range of internet applications. Bank and commercial exchanges are now being carried out online in the form of internet banking and commercial electronic transactions. The level of information transmission is becoming more critical for occurring information leakage, and damages due to such leakages are more significant. User authentication is a necessary security element in the open network environment, and the use of simple authentication information also has some severe problems.

One problem is that it is easy for the attackers to guess passwords whenever the users often choose personal information, such as their ID or telephone number as passwords. The users do this to remember them quickly. Sometimes they use the same password for many web sites. They do this so that they do not have to remember too many passwords. Another problem is that many of the deficiencies of password authentication systems arise from human memory limitations. We know that a maximally secure password with maximum entropy consists of a string having numerous random special characters as long as the system permits. But human memory cannot remember such long as well as complex passwords. Some passwords may be easy to remember (for example, best friends name, pets name, kids name, etc.) but also easy to crack through dictionary searches. Other passwords may be secure against guessing but challenging to recall. Besides, some users tend to create different passwords for their various online accounts. When users create different passwords for different accounts, they need to remember several passwords which may be problematic or confusing for them during use. In this case, for remembering all the passwords, they sometimes keep insecure written records of them. Having a written document of passwords is a terrible idea because this act is not free of password cracking attacks. Eventually, an attacker can easily guess the password.

So, to address this issue, in this paper, I have proposed an automated system to generate user-friendly and robust passwords by combining small letters, capital letters, special symbols and numbers. Later the user can copy the generated password for further usage. Also, user can enter into the password manager by entering master password, in the password manager user can store passwords for various websites/platform with website name, username, and user can also paste his/her generated passwords generated from the password generator. So, user will no longer be needed to remember the password for various accounts, and easily access passwords whenever needed by just entering master password.

# II. LITERATURE REVIEW

Some of the existing methodologies for the Password Manager and Password Manager are described as below,

In this proposed system, Strong Password Generation Based On User Inputs they are generating the passwords by prompting users to provide them with some texts and numbers

(which they can easily remember) as inputs. The generated passwords have ensured the minimum criteria of the password strength. Their generated passwords are different from the passwords of other online random password generators as they are not produced entirely at random. Instead, they are created from the inputs given by the user. [1].

In, “AutoPass: An Automatic Password Generator”,Firstly, existing schemes cause major difficulties for users with a large body of existing passwords, since they are obliged to change them all; AutoPass avoids this through the use of password offsets, allowing continued use of existing passwords. Secondly, the usage of the AutoPass server permits flawless cross-platform working. Thirdly, the use of the Pattern recognition and machine learning which is provided by server statements allows passwords to be automatically generated to satisfy some specific requirements. But still , while AutoPass only works in theory, it remains unverified that the system will actually work in practice. [2].

In “A password generator tool to increase users’ awareness on bad password construction strategies”, the authors are mainly focusing on the use of cybersecurity in making passwords. There is only discussion on why traditional passwords shall not be used , and hoe to implement cybersecurity in the field of passwords. [3].

In this system, “Syntactic Generation of Memorable Passwords," the users are permitted to specify their interests (for example music, movie, colour etc.) and phrases,words or sentences from these interests are used, in combination with one ,two or atmost three numbers and one special symbol, to get memorable and recoverable passwords. This idea is implemented during a software tool called PassGen. PassGen takes, as input user interests, and generate n passwords for the user to settle on from. 20,000 samples of generated passwords. [4].

In "Graphical Passwords Using Images with Random Tracks of Geometric Shapes," they presented a graphical passwordrandom geometric graphical password justified that it indeed is robust against common security attacks such as brute-force search, spyware, shoulder surfing, social engineering, and forgery, etc. They also showed up the images and photos to display user friendliness in both recognition and selection of pass objects from the given images. [5].

In “Cloud Password Manager Using Privacy-Preserved Biometrics” system, the privacy-preserving biometrics (using rigidly-irreversible template protection method) based password manager scheme proposed in this paper enables people to use two factors (a master key and the biometrics) for password binding and releasing in a secure way. Cloud infrastructure is used to synchronize all the password manager clients with the updated encrypted records. [6].

In “Analysis on the Security and Use of Password Managers”, they have gone through over three open-source password managers, each chosen for their own uniqueness, namely, Passbolt, Encryptr and Padlock. This paper just compared three password managers and concluded on the overall security of each password manager using a list of established attacks and development of new potential attacks on such software.[7].

# III. METHODOLOGY

## A. Packages/Modules

1.Tkinter

Tkinter is Python's de-facto standard GUI (Graphical User Interface) package. This framework provides Python users with a simple way to create GUI elements using the widgets found in the Tk toolkit. Tk widgets can be used to construct buttons, menus, data fields, etc. in a Python application.

2.Random

Python Random module is an in-built module of Python which is used to generate random numbers. This module can be used to perform random actions such as generating random numbers, print random a value for a list or string, etc. In this project I have used this module to generate random passwords.

3.PIL

Python Imaging Library is a free and open-source additional library for the Python programming language that adds support for opening, manipulating, and saving many different image file formats. In this project I have used this module so that I could import images and apply them in the GUI.

4.Hashlib

The Python hashlib module is an interface for hashing messages easily. This contains numerous methods which will handle hashing any raw message in an encrypted format. The core purpose of this module is to use a hash function on a string, and encrypt it so that it is very difficult to decrypt it.

1. 5.Functools

Functools module is for higher-order functions that work on other functions. It provides functions for working with other functions and callable objects to use or extend them without completely rewriting them. This module has two classes – partial and partialmethod. In this project I have used Partial class. Partial functions allow us to fix a certain number of arguments of a function and generate a new function.

1. 6.Sqlite3

SQLite is a self-contained, file-based SQL database. SQLite comes bundled with Python and can be used in any of your Python applications without having to install any additional software. In this project I have used it basically for storing the passwords and performing operations on them.

## B. Working

**Password Generator:**

In my methodology, at first, the generator takes input information from the user who is asking for a password. What this information consists of? So, it first asks the user what length of password he is expecting for (from 8 to 30 characters) then the password generator will ask the user about the combination of characters of the password. Whether the user wants numbers, special characters, small letters, or capital letters in his password or whether the user wants the password to be the combination of all the above-mentioned characters. Once the user selects the type of combination, the user just needs to click on 'generate password' button which is provided in the GUI.

Then the system randomly picks the number of characters from the lists provided in the code. Then the password generator applies a randomisation technique generate a password. Password generator appends the 'password' list which was initially empty. And at last the password which is generated is displayed on the screen..! Then, if user wishes to copy the generated password he can click on ‘copy to clipboard’ button which is available on the password generator screen, and if the password is successfully copied the message ‘password was successfully copied’ will be displayed on the screen.

**Password Manager:**

Once the user runs the code for first time of password manager the system will ask the user to enter the master password of his wish(as shown in fig.1.)

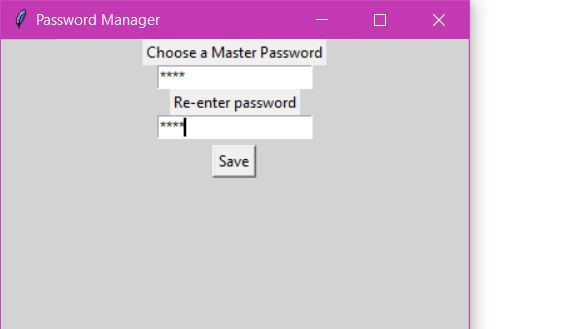


Fig. 1. Master Password Screen Initially

Once the user enters master password the main screen of password manager will appear. On this main screen there will be a button called ‘Add Entries’ which user has to click in order to begin the process of storing the password(as shown in fig.2)

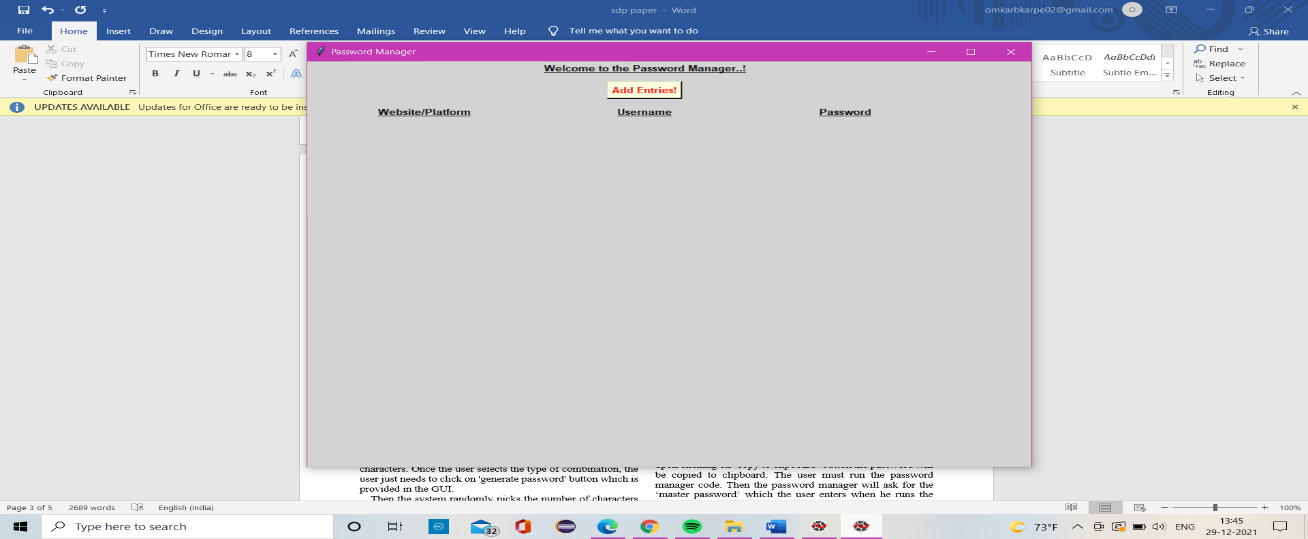


Fig.2. Initial Screen of password manager

Once that button is clicked, the system will ask the user to enter the name of the website for which he wants to store the password. After entering the name of the website/platform, the system will ask the user to enter the username for the website, if it is required. Then system will ask the user to enter the password for the website, where user can either enter the password of his wish or he can simply paste the password which was copied from the password generator.

Now, if user wishes to see the particular password from the password manager, he has to run the once again but this time, the system will ask the user to enter the master password, internally the system will check whether the master password matches with the master password which was earlier entered. If the password matches user will be allowed to enter into the password manager. The user now will be able to see the passwords which he stored earlier. I have also provided the delete button in case if the user wishes to delete the particular entry. On clicking the delete button the system will connect to the database and will delete that particular entry from the database.

# IV. RESULTS AND DISCUSSIONS

Password manager and generator GUI is successfully created. As the user opens the password generator it asks the user for the length of the password (from 8 to 30 characters). Later it asks the user whether the password should contain numbers, special characters, small letters or capital letters. It recommends the user that for strong password at least two options shall be selected as shown in the figure.3. Then upon clicking on ‘Generate Password’ button the password will be generated based on the options selected by the user. Then upon clicking on ‘copy to clipboard’ button the password will be copied to clipboard. The user must run the password manager code. Then the password manager will ask for the ‘master password’ which the user enters when he runs the code for first time. It is shown in Fig 4. Then upon clicking ‘submit’ button the user will be directed to the main screen of password manager where user has to click on ‘add entries’ button for entering the website and its username, then the password manager will ask for the password to be stored, where user can either put his own password or he can paste the password which is copied from the password generator and upon successfully entering the password all the three entries(website/platform, username, password) will be shown. I have also provided the delete button which user can use if he wishes to delete the particular entries. The result from my project is displayed in Figure 3, Figure 4, Figure 5.

Fig.3. Password Generator

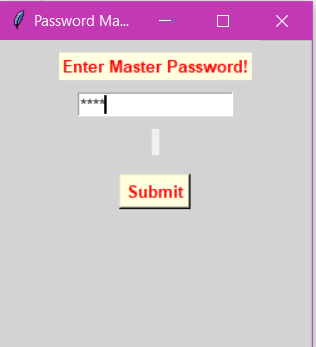


Fig.4. Master Password Screen

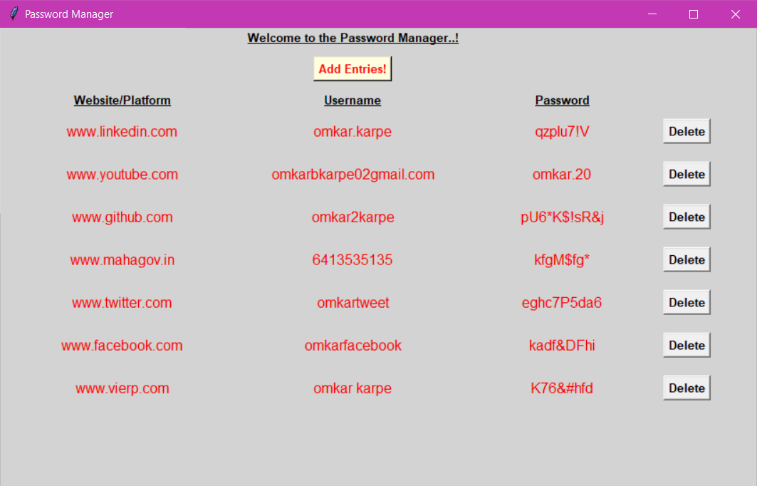


Fig.5. Password Manager

# V. LIMITATIONS

However, there are not many limitations to my project but few limitations to my project are:

* One has to remember the master password in order to get access to his/her password manager.
* If any person somehow gets to know the master password, then he/she may get access to the all the passwords of the user.
* Password generator cannot generate the password of length greater than 30 characters.

# VI. FUTURE SCOPE

In future the system can be upgraded as to:

* Creating an app or a website of the same idea so it would be easier for the user to access the passwords.
* Enhancing security to the master password so that no one would be able to access it, other than user.
* Providing an option such as, “Forgot Master Password”, to retrieve it in case anyone forgets master password.
* Length of the password to be generated could be by user’s choice (of any length), rather than being limited to 30.

# VII. CONCLUSION

In my proposed system, I have tried to implement both password generator and password manager in an effective way. This password generator will not help in generating the random passwords but it will also store the passwords so that if user forgets the password for any website he can access the password manager, by entering the master password. The master password is like the key to the password manager, the user must remember the master password. In future I am planning to develop this project by implementing this to website or app. I am also looking for an alternative if user forgets the master password. So, due to this password generator and password manager, now , user no longer needs to remember his username or password for various platforms because now he can easily store the usernames and passwords..!

## ACKNOWLEDGMENT

I would like thank my guide Proff. Abha Marathe Mam for her support and wonderful guidance, also I would give a big thanks to Vishwakarma Institute of Technology as well for providing me with this opportunity.

## REFERENCES

1. F. Z. Glory, A. Ul Aftab, O. Tremblay-Savard and N. Mohammed, "Strong Password Generation Based On User Inputs," *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, 2019.
2. F. Al Maqbali and C. J. Mitchell, "AutoPass: An automatic password generator," 2017 International Carnahan Conference on Security Technology (ICCST), 2017.
3. P. Tsokkis and E. Stavrou, "A password generator tool to increase users' awareness on bad password construction strategies," 2018 International Symposium on Networks, Computers and Communications (ISNCC), 2018.
4. A. Ade-Ibijola and B. Ogbuokiri, "Syntactic Generation of Memorable Passwords," 2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC), 2019.
5. P. Lin, L. Weng and P. Huang, "Graphical Passwords Using Images with Random Tracks of Geometric Shapes," 2008 Congress on Image and Signal Processing, 2008.
6. C. Luevanos, J. Elizarraras, K. Hirschi and J. Yeh, "Analysis on the Security and Use of Password Managers," 2017 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT), 2017.
7. B. Yang, H. Chu, G. Li, S. Petrovic and C. Busch, "Cloud Password Manager Using Privacy-Preserved Biometrics," 2014 IEEE International Conference on Cloud Engineering, 2014.