A Mini Project Synopsis on

Password Manager

S.E. - I.T Engineering

Submitted By

Shweta Bhutada 21104007

Manjiri Gole 21104006

Akshata Nalavade 21104003

Under The Guidance Of

Prof. Manasi Choche

DEPARTMENT OF INFORMATION TECHNOLOGY

A.P.SHAH INSTITUTE OF TECHNOLOGY

G.B. Road, Kasarvadavali, Thane (W), Mumbai-400615

UNIVERSITY OF MUMBAI

Academic year : 2022-23

CERTIFICATE

This to certify that the Mini Project report on Password Manager has been submitted by Shweta Bhutada(21104007), Manjiri Gole(21104006) and Akshata Nalavade(21104003) who are a Bonafede students of A. P. Shah Institute of Technology, Thane, Mumbai, as a partial fulfilment of the requirement for the degree in **Information Technology**, during the academic year **2022-2023** in the satisfactory manner as per the curriculum laid down by University of Mumbai.

Prof. Manasi Choche

Guide

Dr. Kiran Deshpande
Head Department of Information Technology

Dr. Uttam D.Kolekar
Principal

External Examiner(s)

1.

2.

Place:A.P.Shah Institute of Technology, Thane

Date:

ACKNOWLEDGEMENT

This project would not have come to fruition without the invaluable help of our guide **Prof. Manasi Choche**. Expressing gratitude towards our HoD, **Dr. Kiran Deshpande,** and the Department of Information Technology for providing us with the opportunity as well as the support required to pursue this project. We would also like to thank our teacher Ms.Manasi Choche who gave us her valuable suggestions and ideas when we were in need of them. We would also like to thank our peers for their helpful suggestions.

TABLE OF CONTENTS

1. Introduction. 1

    1.1. Purpose 1

    1.2. Objectives. 2

    1.3. Scope 2

2. Problem Definition… 3

3. Proposed System…. 4

    3.1. Features and Functionality…. 4

4. Project Outcomes. 5

5. Software Requirements 6

6. Project Design. 7

7. Project Scheduling. 11

8. Conclusion. 12

References

Chapter 1

Introduction

Data breaches are on the rise, which are caused by weak, reused or stolen passwords. Doing nothing could mean losing everything. That’s why password security has never been more critical for individuals and businesses. Passwords are difficult to remember, and users have many accounts that require passwords. This causes users to choose memorable but weak passwords and then reuse them, which creates major security problems. We have proposed a method for users to only need to remember one password that they use to access all their other passwords from any device at any time. When you use this software, the passwords are encrypted, and you use a single master password to access them. Depending on the tool being used, these passwords are stored on a securely. You can also view the database of other passwords for various sites and apps.

1.1. Purpose:

1. Password managers encourage users to create strong, unique passwords and regularly change them, which is important for good password hygiene. This helps protect against password-based attacks.

2. Users no longer need to remember numerous passwords, reducing the burden of managing multiple logins. Auto-fill features make it easy to log in to websites, saving time and reducing the risk of typing errors.

3. Password managers keep sensitive information private and secure, helping to protect users' privacy online.

4. Desktop-based password managers can be the safest, but that depends solely on the user.
5. These password managers store your data locally, on one of your devices. That device doesn't have to be connected to the internet, so there might be nearly zero chances of hacking into it**.**

1.2. Objectives:

1. Convenience: With a password manager, users only need to remember one master password to access all of their other passwords. This can save time and reduce the stress of trying to remember multiple passwords.
2. Security: Password managers can generate strong, unique passwords for each account, making it much harder for hackers to guess or crack them. This can help prevent identity theft and other types of cyber attacks.
3. Organization: Password managers can help users keep track of all their passwords in one place, making it easier to find and update them when needed.

1.3 Scope:

1. Safe and Secure: Reliable password managers are very hard to hack. Strong encryption is offered by password managers, acting as a powerful deterrent to online criminals.
2. Easy accessibility and managing: Logging onto accounts is simple. You can also launch websites directly from the password manager instead of navigating to the site yourself.
3. One master password to access your credentials: A password manager stores all of your passwords in a single vault using one strong master password. The master password is the only password you will need to remember to access your vault.

Chapter 2

Problem Definition

Passwords are a critical aspect of our digital lives. We use them to access online accounts, protect sensitive information, and secure our personal data. However, with the increasing number of online accounts and services we use, remembering unique and complex passwords for each account can be a daunting task. Users had to remember the list of passwords for different accounts on the internet. The user had to manually maintain a list of all usernames and passwords. This task was very tedious. In cases where privacy for user accounts was required, it was difficult to manually maintain this list of passwords. As a result, many people resort to using the same weak password across multiple accounts or write them down on insecure notes, which puts their accounts at risk of being hacked. Password Manager is an GUI based application that allows users to store unique, complex passwords for each account they have. A password manager is a program that houses all your passwords, as well as other information, in one convenient location with one master password

Chapter 3

Proposed System

3.1. Features and Functionality:

Password Manager is an GUI based application. It is created in Python using Tkinter and Mysql database to manage passwords for several application. Python Features and methods are used to implement this project. While it is important to use strong passwords and to use different passwords on each site, it can be a difficult task to remember all them. With a password manager, you simply enter the GUI app, provide the master password you set for the password manager in that software, then log in to the GUI app and the username and password will be stored for you.

Some of the features are listed below:

Feature 1: Registration/Login

This form allows new users to create an account by providing basic information such as their name, email address and password. This form allows users to access their account by entering their username/email and password.

Feature 2: OTP Verification

The OTP verification process typically begins with the user entering their email address associated with their password manager account. The password manager then generates a unique OTP code that is sent to the user's email.

Feature 3: Master Key

The user creates the master key during the initial setup of the password manager. The master key should be unique and strong, consisting of a combination of uppercase and lowercase letters, numbers, and symbols. Provides an additional layer of security to protect all the user's passwords.

Feature 4: Password categories

Help users organize their passwords based on different criteria.

So the primary purpose of this project to make Password Manager application user-friendly

Chapter 4

Project Outcomes

1. Increased productivity: Password managers can save users time and hassle by eliminating the need to manually enter login credentials and reset forgotten passwords.
2. Accessibility: Password managers can be accessed across multiple devices and platforms, making it easy for users to manage their passwords from anywhere.
3. Peace of mind: With a password manager, users can rest assured that their accounts are secure and that they are doing their part to protect their personal information.

Chapter 5

Software Requirements

For this project we used different software and technologies.

The main software's used were:

1. PyCharm

2. MYSQL

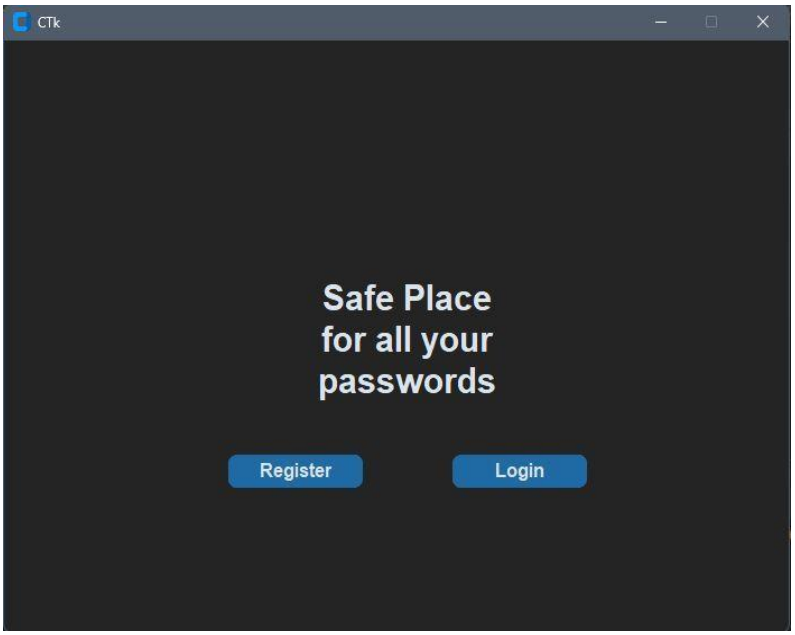
PyCharm was used to create the GUI and connecting the front end and the backend of the website.

MYSQL was used to create the database for the website.

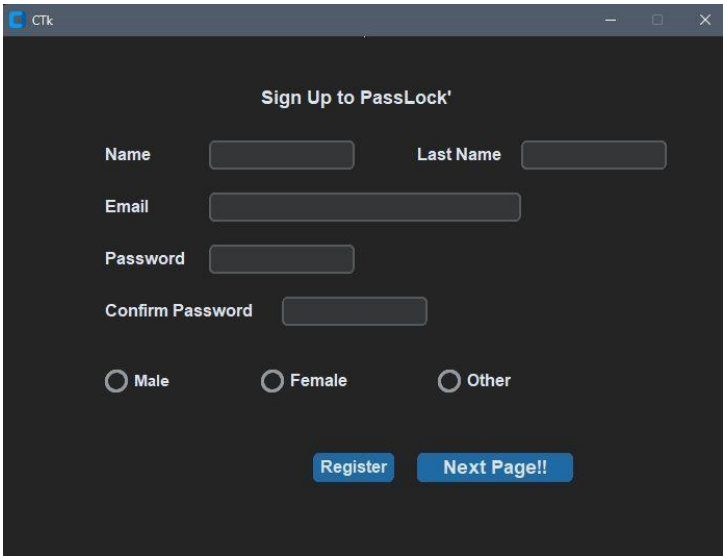
Chapter 6

Project Design

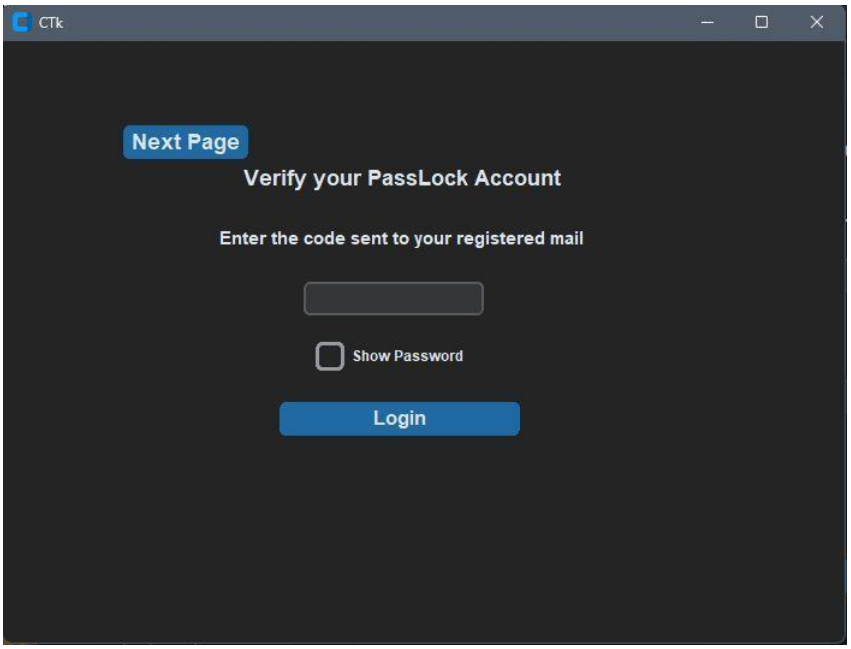
6.1 App Introduction Page



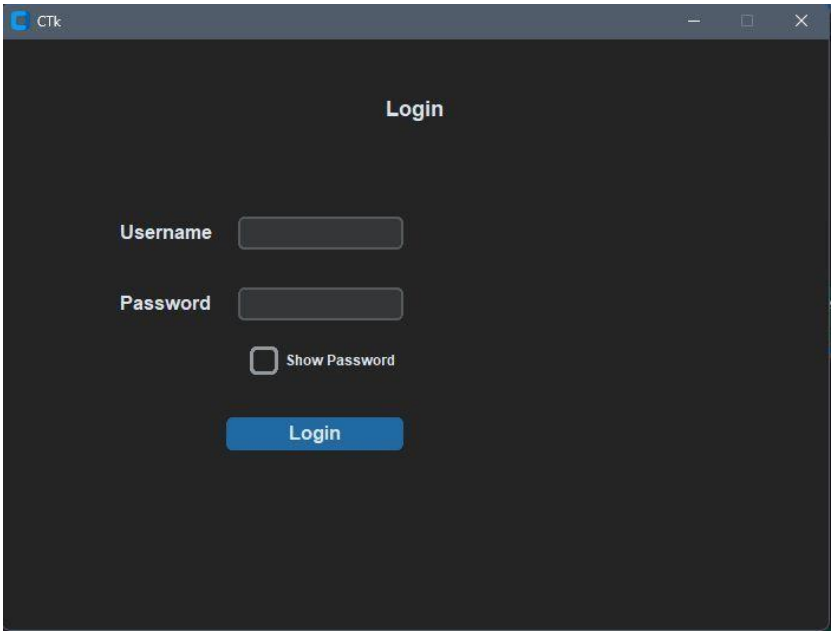
6.2 Registration Page



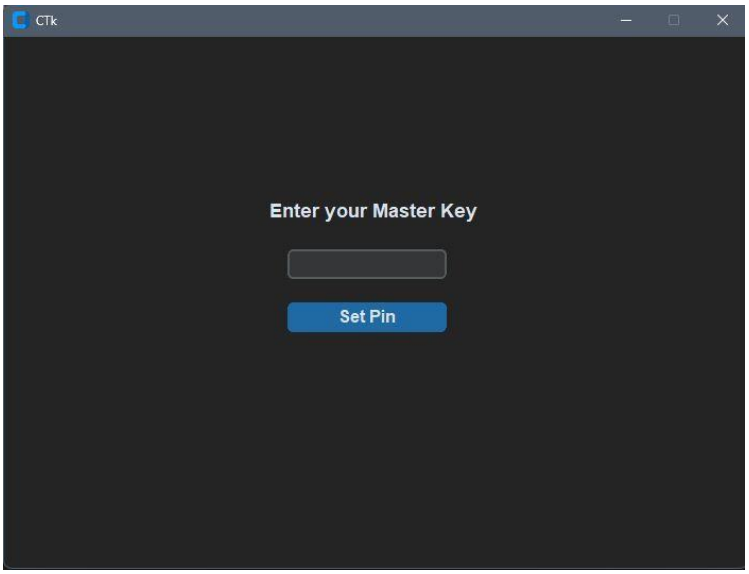
6.3 OTP Verification Page



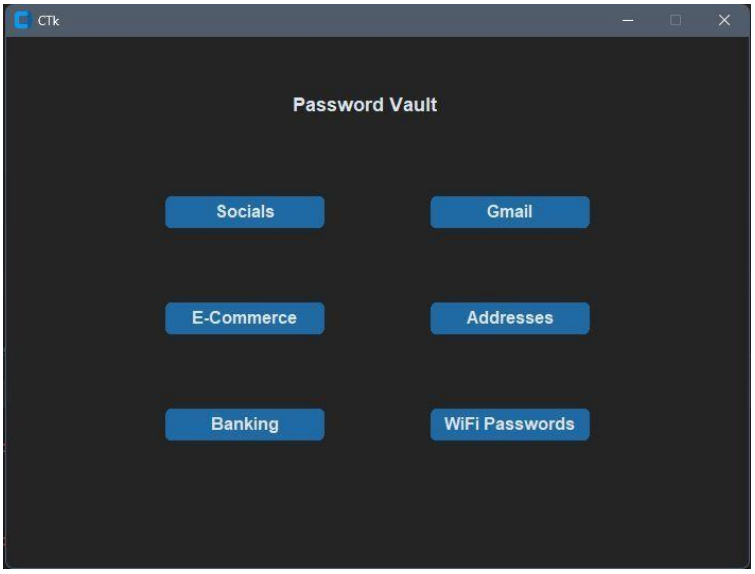
6.4 Login Page



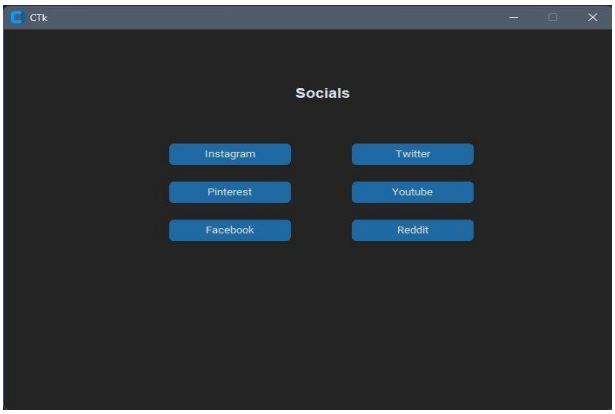
6.5 Master Key Page



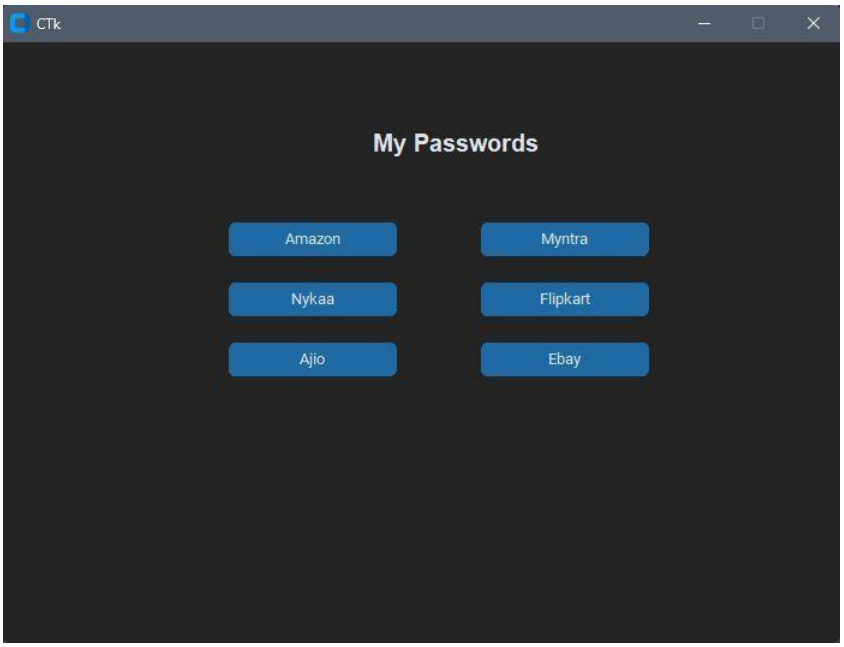
6.6 Password Categories Page



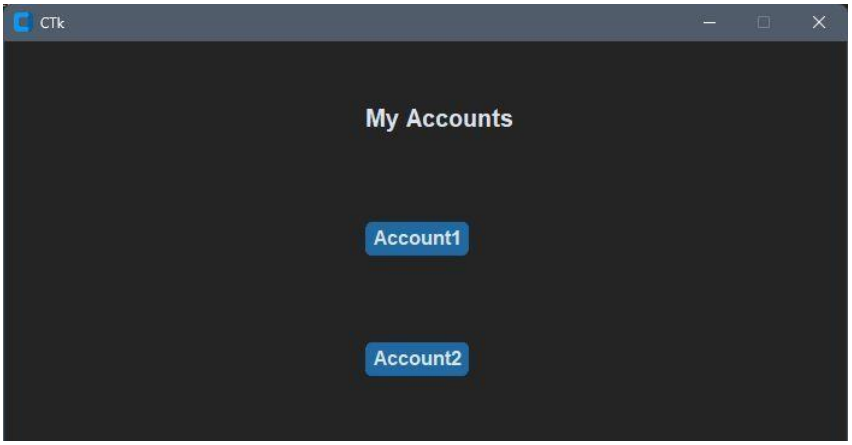
6.7 Socials Page



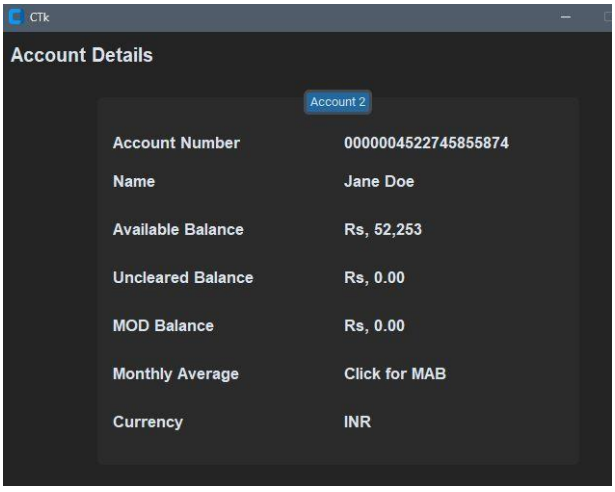
6.8 Ecommerce Page



6.9 Banking Detail Page



6.10 Banking Detail Page 2



Chapter 7

Project Scheduling Template

Sr. No	Group Member	Time duration	Work to be done
1	Manjiri Gole	1st week of january	Implementing 1st module/ functionality Learnt basics of PyCharm and followed Tkinter tutorials. Implemented GUI using Tkinter
		2nd week of january	Testing 1st module GUI ready along with the feedbacks of guide and implemented the task. Added some new features as per the feedback.
2	Shweta Bhutada	3rd week of january	Implementing 2nd module/ functionality Implementation of Database Connectivity using Python. Learnt basics of PyCharm and MySQL.
3	Akshata Nalavade	By the end of march month	Implementing 3rd module/ functionality GUI Implementation with Tkinter. Learnt basics of connectivity Report Making

Chapter 8

Conclusion

In today's digital age, the use of password managers has become increasingly important for individuals to ensure their online security. Password managers offer users a simple yet effective way to securely store and manage their passwords, generating strong, unique passwords for each account. This reduces the risk of cyber attacks such as identity theft and data breaches, which can have devastating consequences. Password managers also offer convenience, allowing users to access their passwords across multiple devices and simplifying the login process. With password managers, users can keep their digital identities safe, organize their passwords more efficiently, and share them securely with trusted individuals. Overall, password managers are a valuable tool that can significantly improve the online security and digital life of individuals, making them an essential component of anyone's digital toolkit.

References

https://youtu.be/z73PyNDgVyQ

https://youtu.be/hkhyKJj28Ac

https://youtu.be/57HpogJv9ZQ