**A**

**MAJOR PROJECT REPORT**

**ON**

PASSWORD MANAGER

Major project report submitted in the partial fullfillment of the requirement of the course

***Bachelor of Technology***

In

COMPUTER SCIENCE AND ENGINEERING

(ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING)

Submitted By

**R.AJAY 22BH1A6683**

**P.PAVAN 22BH1A6677**

**NARESH 22BH1A6672**

**M.DIBYA RANJAN 23BH6A6601**

**V.VARUN KUMAR 22BH1A6696**

***Under the guidance of***

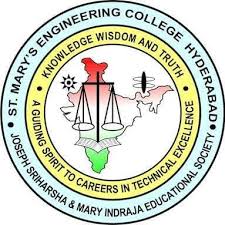
**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

*(ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING)*

**St.Mary’s Engineering Collage**

(Affiliated to JNTU, Hyderabad)

Deshmukhi(V),Pochampally(M), Nalgonda District-508284



**JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY**

HYDERABAD -500072

(2023-2024)

**PASSWORD MANAGER**

***ABSTRACT***

Passwords are essential for keeping our online accounts secure, but it can be difficult to keep track of them all. A password manger can help by storing all of your passwords in one place and encrypting them so that they are safe from unauthorized access.

This project will develop a password manger in python. The password manger will use are database to store passwords and will encrypt them using the AES-256 encryption algorithm. The password manager will also have a graphical user interface (GUI) that will allow users to easily add, edit, and delete passwords.

The password manager will be developed using the following Python libraries:

* PyQt5: This library will be used to create the GUI.
* SQLAICHEMY: This library will be used to interact with the database.
* pycryptodome: This library will be used to encrypt and decrypt passwords.

The password manager will be tested using the following methods:

Unit testing:

The individual components of the password manager will be tested to ensure that they work as expected.

Integration testing:

The different components of the password manager will be tested together to ensure that they work together correctly.

System testing:

The password manager will be tested as a whole to ensure that it meets all of the requirements.

-The password manager will be a valuable tool for anyone who wants to keep their online accounts secure. It will be easy to use and will provide a high level of security for passwords.

**CERTIFICATION**

This is to certify that project report entitled “**PASSWORD MANAGER**” is bonafied work carried

out in the 2nd year in 2nd semester by **R.AJAY (22BH1A6683),** **P.PAVAN (22BH1A6677), NARESH (22BH1A6672), M.DIBYA RANJAN (23BH6A6601), V.VARUN KUMAR (22BH1A6696)**. In partial fulfilled award of Bachelor of Technology in **CSE (Artificial Intelligence & Machine Learning) from** St. Mary’s Engineering College during the academic year 2023-2024.

**INTERNAL GUIDE**  **HEAD OF THE DEPARTMENT**

Dr. k Suresh Kumar, M.Tech, PH. D

Dept. of CSE(AIML)

**EXTERNAL EXAMINER**

**ACKNOWLEDGEMENT**

The satisfaction that accompanies the successful completion of this project would be incomplete without the mention of the people who made it possible. We consider it as a privilege to express our gratitude and respect to all those who guided us in the completion of the project.

We are thankful to our internal guide **Mr . B. Murali Krishna, Assistant Professor**,

in the St. Mary's Engineering College for having been a source of encouragement and for insisting on vigor to do this project work.

We are obliged to **Dr . K Suresh Kumar, Head of the Department of CSE (Artificial Intelligence Machine Learning)**, St. Mary's Engineering College for his guidance and suggestions throughout the project work.

We take this opportunity to express a deep sense of gratitude to **Dr . T.N. Srinivas Rao, Principal** of St. Mary's Engineering College for allowing us to do this project and for this affectionate encouragement in presenting this project work.

We convey our sincere thanks to **Sri Rev. K.V.K RAO, Chairman** of St. Mary's Engineering College for giving us a learning environment to grow ourselves personally as well as professionally.

We would like to express our thanks to all staff members who have helped us

directly and indirectly in accomplishing this project work. We also extended our sincere thanks to our parents and friends for their moral support throughout the project work.

Above all, we thank god almighty for his manifold mercies in carrying out this project work successfully.

**R. AJAY -22BH1A6683**

**P. PAVAN -22BH1A6677**

**NARESH -22BH1A7772**

**M. DIBYA RANJAN -23BH6A6601**

**V. VARUN KUMAR -22BH1A6696**

**DECLARATION**

This is a certify that the work report in this titled. “**PASSWORD MANAGER**”, submitted to the Department of **CSE (Artificial Intelligence & Machine Learning)**,

**St. Mary’s Engineering College** in fulfilment if degree for the award of Bachelor of Technology, is a Bonafide work done by us. No part of this is copied from books, journals, or the internet and wherever the portion is taken , the dame has been duly referred to int text.

The reported results the same has been on the project work entity done by us and not copied from any other sources.

Also, we declare that the matter embedded in this has not been submitted by us in full or partially there for the award of any degree from any other institution or university previously .

**R. AJAY -22BH1A6683**

**P. PAVAN -22BH1A6677**

**NARESH -22BH1A7772**

**M. DIBYA RANJAN -23BH6A6601**

**V. VARUN KUMAR -22BH1A6696**

**INTRODUCTION :**

A password manager is a software application designed to store and manage online credentials securely. It helps users create, retrieve, and store complex passwords for their online accounts, thus reducing the risk of password-related security breaches. Here are the main features and benefits of using a password manager:

1. **Security:** Password managers encrypt your passwords, ensuring that only you can access them.

2. **Convenience:** They auto-fill login forms and can generate strong, unique passwords for each of your accounts, eliminating the need to remember multiple passwords.

3**. Organization:** Password managers keep all your login information in one place, making it easy to manage and update passwords as needed.

4. **Syncing Across Devices:** Many password managers can sync your passwords across multiple devices, so you have access to them wherever you go.

5. **Additional Features:** Some password managers offer additional features like secure notes, two-factor authentication (2FA) integration, and alerts for potential security breaches.

Popular password managers include LastPass, 1Password, Dashlane, and Bitwarden. They offer various plans, including free versions and premium subscriptions with enhanced features.

**Key features of a password manager typically include:**

1. **Password Storage and Management**: Securely stores and organizes passwords.

2. **Autofill:** Automatically fills in login forms for websites and applications.

3**. Password Generator:** Creates strong, unique passwords.

4**. Encryption:** Encrypts stored passwords to protect against unauthorized access.

5. **Cross-Platform Syncing:** Syncs passwords across multiple devices and platforms.

6. **Two-Factor Authentication (2FA):** Adds an extra layer of security by requiring a second form of verification.

7. **Password Sharing:** Securely shares passwords with trusted contacts.

8. **Security Alerts:** Notifies users of potential security breaches or weak passwords.

9. **Secure Notes:** Stores sensitive information like credit card details, secure notes, and other personal information.

10**. Audit and Reports:** Analyzes the strength of stored passwords and provides security reports.

11. **Biometric Logins:** Supports fingerprint or facial recognition for accessing the password manager.

12**. Integration with Browsers and Apps:** Seamlessly integrates with web browsers and mobile apps for ease of use.

13. **Backup and Recovery:** Offers options for securely backing up and recovering passwords.

14**. Custom Fields:** Allows adding custom fields for specific login requirements or additional information.

**Problem Statement:**

In today's digital age, individuals and organizations are required to manage numerous online accounts, each with unique usernames and passwords. As the number of these accounts grows, so does the complexity of managing them securely. Common problems associated with password management include:

1. **Password Fatigue:** Users often struggle to create, remember, and manage a large number of complex passwords.

2. **Security Risks:** Using weak or repeated passwords across multiple accounts increases vulnerability to cyberattacks.

3. **Inconvenience:** Frequent password resets and account lockouts due to forgotten passwords can be frustrating and time-consuming.

4**. Data Breaches:** A single compromised password can lead to unauthorized access to multiple accounts, causing significant damage.

**Objective:**

Develop a robust, user-friendly password manager application that addresses the above problems by providing a secure and efficient solution for managing passwords. The application should offer the following features:

1**. Secure Password Storage:** Encrypt and store passwords securely, ensuring that only the user can access their credentials.

2. **Password Generation:** Provide a password generator that creates strong, unique passwords for each account.

3**. Auto-fill and Auto-save:** Automatically fill in login credentials on websites and save new passwords when accounts are created or updated.

4. **Cross-Platform Sync:** Ensure that users can access their passwords across multiple devices (e.g., computers, smartphones, tablets).

5. **User Authentication:** Implement multi-factor authentication to enhance security when accessing the password manager.

6**. User-friendly Interface:** Design an intuitive interface that makes it easy for users to manage their passwords without technical expertise.

**Expected Outcomes:**

1**. Enhanced Security:** Reduce the risk of account breaches by encouraging the use of strong, unique passwords for each account.

2. **Improved User Experience**: Simplify the process of managing passwords, reducing frustration and saving time for users.

3. **Increased Adoption:** Encourage more individuals and organizations to adopt secure password management practices through a user-friendly application.

**Code:**

import tkinter as tk

from tkinter import messagebox

def add():

# accepting input from the user

username = entryName.get()

# accepting password input from the user

password = entryPassword.get()

if username and password:

with open("passwords.txt", 'a') as f:

f.write(f"{username} {password}\n")

messagebox.showinfo("Success", "Password added !!")

else:

messagebox.showerror("Error", "Please enter both the fields")

def get():

# accepting input from the user

username = entryName.get()

# creating a dictionary to store the data in the form of key-value pairs

passwords = {}

try:

# opening the text file

with open("passwords.txt", 'r') as f:

for k in f:

i = k.split(' ')

# creating the key-value pair of username and password.

passwords[i[0]] = i[1]

except:

# displaying the error message

print("ERROR !!")

if passwords:

mess = "Your passwords:\n"

for i in passwords:

if i == username:

mess += f"Password for {username} is {passwords[i]}\n"

break

else:

mess += "No Such Username Exists !!"

messagebox.showinfo("Passwords", mess)

else:

messagebox.showinfo("Passwords", "EMPTY LIST!!")

def getlist():

# creating a dictionary

passwords = {}

# adding a try block, this will catch errors such as an empty file or others

try:

with open("passwords.txt", 'r') as f:

for k in f:

i = k.split(' ')

passwords[i[0]] = i[1]

except:

print("No passwords found!!")

if passwords:

mess = "List of passwords:\n"

for name, password in passwords.items():

# generating a proper message

mess += f"Password for {name} is {password}\n"

# Showing the message

messagebox.showinfo("Passwords", mess)

else:

messagebox.showinfo("Passwords", "Empty List !!")

def delete():

# accepting input from the user

username = entryName.get()

# creating a temporary list to store the data

temp\_passwords = []

# reading data from the file and excluding the specified username

try:

with open("passwords.txt", 'r') as f:

for k in f:

i = k.split(' ')

if i[0] != username:

temp\_passwords.append(f"{i[0]} {i[1]}")

# writing the modified data back to the file

with open("passwords.txt", 'w') as f:

for line in temp\_passwords:

f.write(line)

messagebox.showinfo(

"Success", f"User {username} deleted successfully!")

except Exception as e:

messagebox.showerror("Error", f"Error deleting user {username}: {e}")

if \_name\_ == "\_main\_":

app = tk.Tk()

app.geometry("560x270")

app.title("GeeksForGeeks Password Manager")

# Username block

labelName = tk.Label(app, text="USERNAME:")

labelName.grid(row=0, column=0, padx=15, pady=15)

entryName = tk.Entry(app)

entryName.grid(row=0, column=1, padx=15, pady=15)

# Password block

labelPassword = tk.Label(app, text="PASSWORD:")

labelPassword.grid(row=1, column=0, padx=10, pady=5)

entryPassword = tk.Entry(app)

entryPassword.grid(row=1, column=1, padx=10, pady=5)

# Add button

buttonAdd = tk.Button(app, text="Add", command=add)

buttonAdd.grid(row=2, column=0, padx=15, pady=8, sticky="we")

# Get button

buttonGet = tk.Button(app, text="Get", command=get)

buttonGet.grid(row=2, column=1, padx=15, pady=8, sticky="we")

# List Button

buttonList = tk.Button(app, text="List", command=getlist)

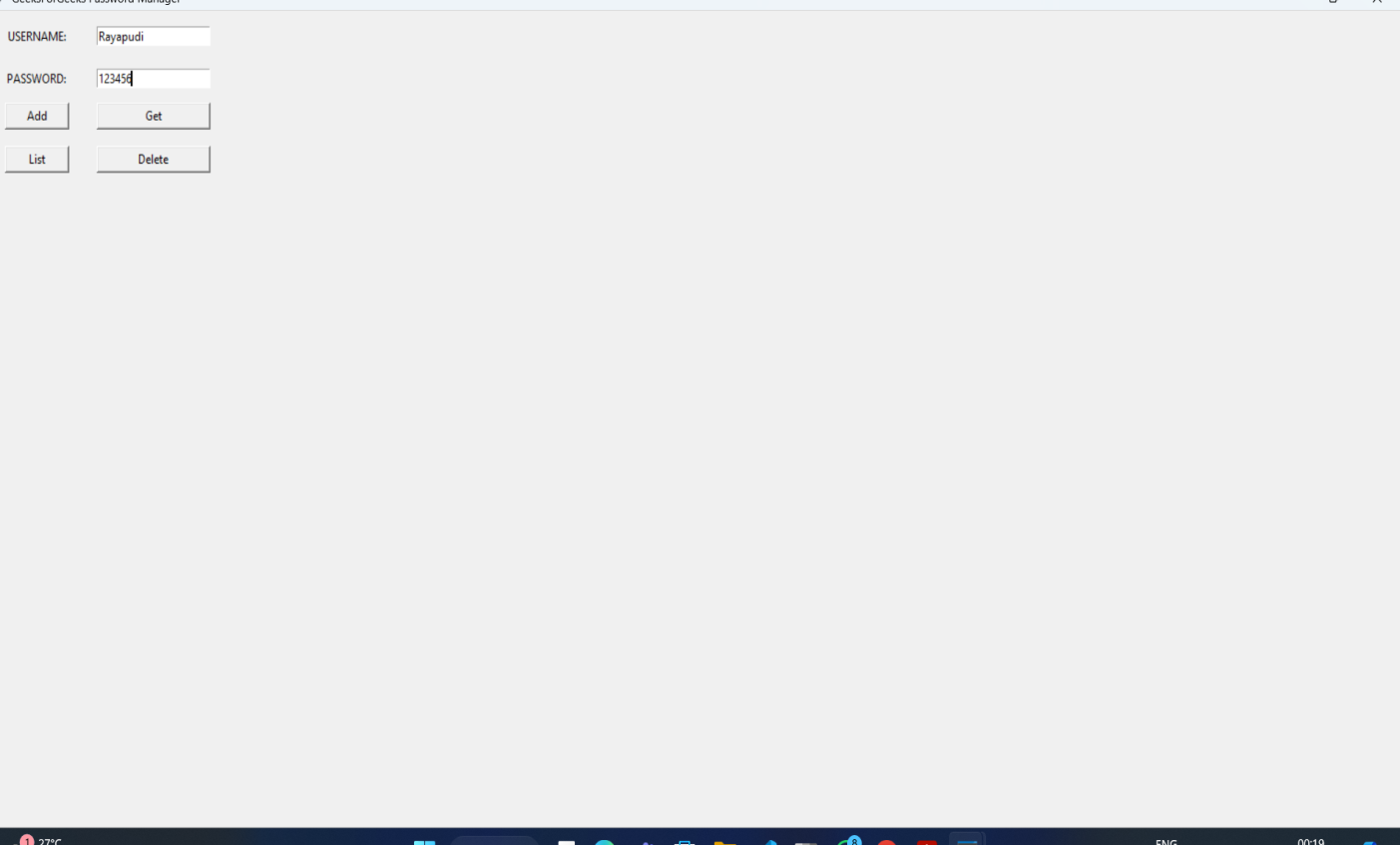
buttonList.grid(row=3, column=0, padx=15, pady=8, sticky="we")

# Delete button

buttonDelete = tk.Button(app, text="Delete", command=delete)

buttonDelete.grid(row=3, column=1, padx=15, pady=8, sticky="we" app.mainloop()

**Output:**

****

**Conclusion:**

**Using a password manager is highly recommended for several reasons:**

1. **Security:** Password managers generate and store strong, unique passwords for each of your accounts, reducing the risk of password reuse and weak passwords that are easily hacked.

2. **Convenience:** They save you from remembering multiple complex passwords, as you only need to remember the master password for the manager itself.

3. **Organization:** Password managers often offer features like secure storage for sensitive information, automatic form filling, and easy access to your passwords across multiple devices.

4. **Time-saving:** They can automatically log you into websites and apps, saving you time and effort.

5. **Reduced Phishing Risk:** Password managers often recognize legitimate sites, helping to protect you from phishing attacks by not auto-filling login credentials on suspicious sites.

6. **Enhanced Security:** Password managers generate and store complex, unique passwords for each of your accounts, significantly reducing the risk of hacking.

7. **Convenience:** They save you from having to remember multiple passwords, making it easier to use different passwords for different sites.Centralized

8. **Management:** You can access all your passwords from one secure location, usually protected by a strong master password.

9. **Additional Features:** Many password managers offer features like secure notes, autofill for login forms, and alerts for potential security breaches.

Overall, using a password manager enhances your online security and simplifies managing your passwords and sensitive information.

**END...**