

PARSHVANATH CHARITABLE TRUST'S
A.P. Shah Institute of Technology
Thane, 400615

Academic Year: 2022-23
Department of Computer Engineering

**CSL304 SKILL BASED LAB COURSE: OBJECT ORIENTED
PROGRAMMING WITH JAVA**

Mini Project Report

- **Title of Project** : Password manager
- **Year and Semester** : S.E. (Sem III)
- **Group Members Name and Roll No.** : Advait Desai (24)
Atharv Darekar(23)
Tejas Bhandary(14)

Table of Contents

Sr. No.	Topic	Page No.
1.	Problem Definition	3
2.	Introduction	4
3.	Description	5
4.	Implementation details with screen-shots (stepwise)	7
5.	Learning Outcome	11

Problem Definition

A password manager is a computer program that allows users to store, generate, and manage their passwords for local applications and online services.

In this today's world, where everything processes online, we sign up to various apps which fulfill our every needs, and this leads in making lots of passwords for every single app. And in this digital world where any small and easy password can be easily accessible to anyone, we tend to keep difficult ones to keep our data safe and secure. We as humans forget various things and so the passwords we keep for different apps and then we have to go through some tedious tasks to rechange our passwords, and hence we came up with Password Manager, which will keep your sign-up data safe and secure from others.

Password managers don't just store your passwords, they help you generate and save strong, unique passwords when you sign up to new websites. That means whenever you go to a website or app, you can pull up your password manager, copy your password, paste it into the login box, and you're in.

Introduction

A password manager is a computer program that allows users to store, generate, and manage their passwords for local applications and online services.

A password manager is a computer program that allows users to store, generate, and manage their passwords for local applications and online services.

Password managers are applications that serve as the solution for maintaining a large number of passwords and account information. They store the login information of the various accounts and automatically enter them into the forms. This helps in the prevention of hacker attacks like keystroke logging and it prevents the need to remember multiple passwords.

Password managers enable the use of strong and unique passwords for each online account and provide an efficient way to manage all the passwords. The login information is encrypted and stored in either the local memory of the user's system or in cloud storage. Portable password manager applications installed in mobile devices can also be used as a way to manage and remember passwords anywhere and use them on shared systems.

Password managers usually incorporate some additional features like automatic form filling and password generation. The automatic form filling feature fills in the login information for a particular URL whenever it loads, and thus reduces manual errors and protects systems from hacker attacks such as keylogging. As password managers can identify the right URL for a particular login ID and password pair automatically, they are capable of protecting credentials from phishing sites. The automatic password generation feature available in certain password managers helps to create strong, unique and random passwords for each account.

Some of the basic types of password managers are:

- Web browser-based
- Cloud-based
- Desktop
- Portable
- Stateless

Other types of password managers include online password managers and security token password managers used in smart cards and other multi-factor authentication applications.

Description

Today's digitalized corporate space relies heavily on passwords for every service, whether it's something as simple as marking daily attendance or as sensitive as accessing clients' unmasked financial details. However, even the most powerful executive is only human, and it's only a matter of time before remembering numerous passwords for various corporate portals becomes impossible.

Things get even more difficult on the personal front. An average user has different passwords for their email, online shopping, internet banking, social media channels, and several other digital services. According to a 2020 research study the average person has a hundred passwords to remember.

Using a password manager is one of the best ways to stay secure online, and it's easier to get set up than you may think. You might think it could be more trouble than it's worth, but you really need to create a unique password constructed out of capital and lowercase letters, numbers and symbols for each of your online accounts. (Yes, using "password123" for everything isn't going to cut it.) Though it may be tempting, using one easy-to-remember code across all of your accounts can jeopardize your online security – and you definitely don't want to make yourself an easy target for cybercriminals. Password managers are vital tools that can help you stay safe online and be more digitally secure by simplifying the process of using strong passwords.

The objective of this Password Management System is to manage passwords for different accounts on the internet. The user shall be able to save all the username and passwords information of the accounts he holds on the internet using this application. These details shall be saved in the database in encrypted format. This will help the user to remember different usernames and passwords for accounts on the internet. The user shall be able to add account, edit and delete account using the system. The user has to login to the system in order to use this tool. It takes user login and password.

A password manager Is a service that stores your passwords as well as other data like credit card numbers, bank account information and identification documents in a secure, encrypted environment. Bad password habits are dangerous for your digital security. Using weak passwords makes your accounts easy to crack, and reusing passwords leaves you open to credential stuffing attacks that can compromise accounts that share the same password.

We are creating a password manager using the java program. That will help users to save passwords and be free from the worry of forgetting passwords. We have created the program using java GUI so that the program is more interactive and more user-friendly.

This program has an option for adding new passwords and also deleting a password user interface is easy to understand there are two tabs one shows the password and another has the option of adding and deleting the password.

The program has a database it can store the data ie. user name password and shows the user. Today there are a number of software that provide password management System.

Implementation details with screen-shots (stepwise)

This application is called Password Manager in which The passwords list will be stored in the form of arrays.

Basically, we are using swing and awt ,they are used because:

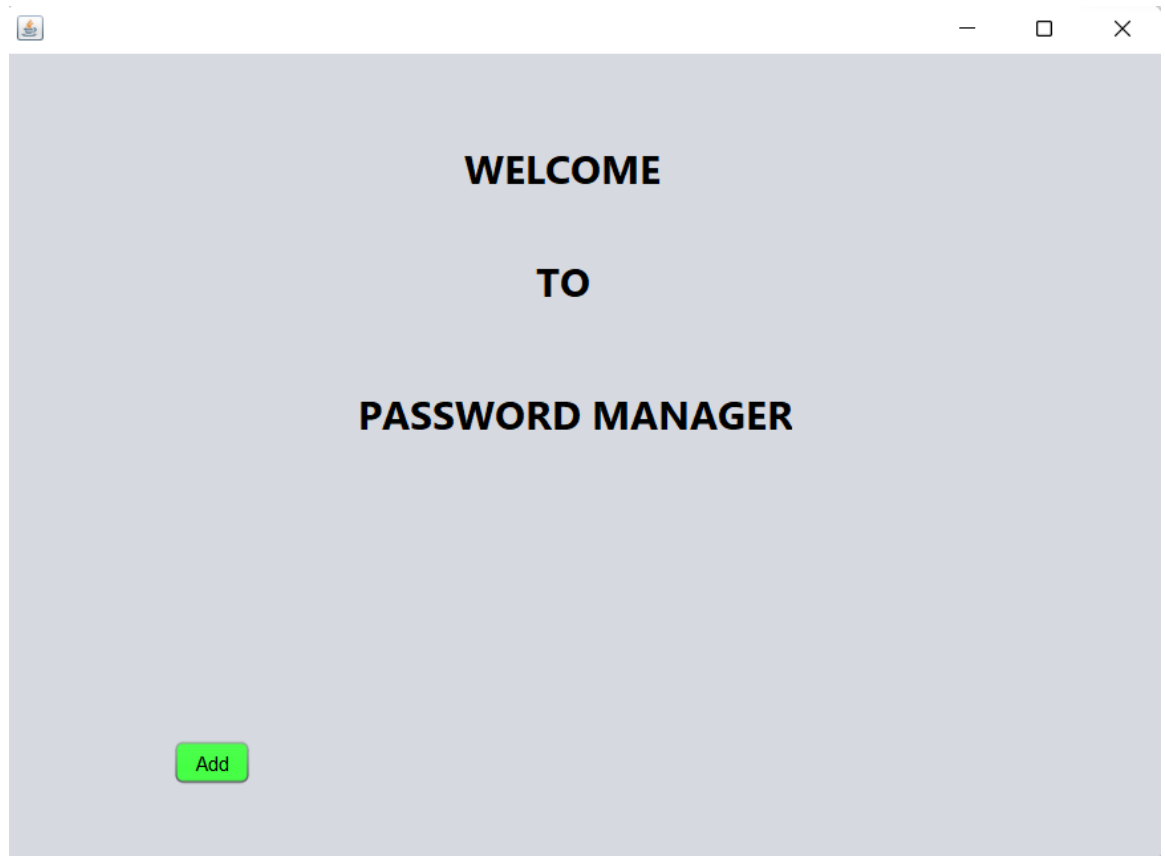
Swing: Java Swing tutorial is a part of Java Foundation Classes (JFC) that is used to create window-based applications. It is built on AWT.

AWT (Abstract Window Toolkit): It is a set of application program interfaces used by Java programmers to create graphical user interface objects, such as buttons, scroll bars, and windows.

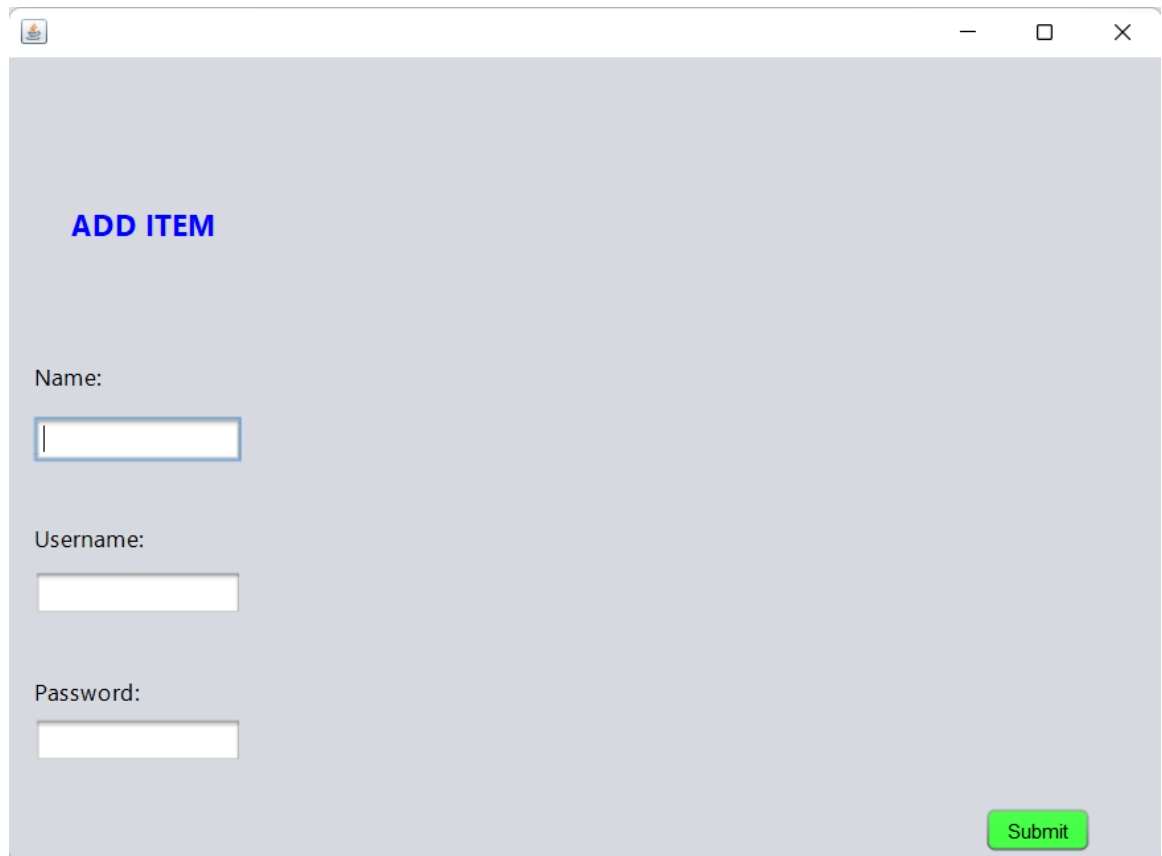
We have used different classes like:

- JButton: The JButton class is used to create a labeled button that has platform independent implementation.
- JLabel: The object of JLabel class is a component for placing text in a container.
- JRadioButton: The JRadioButton class is used to create a radio button.
- JOptionButton: The JOptionPane class is used to provide standard dialog boxes such as message dialog box, confirm dialog box and input dialog box.
- JScrollbar: The object of JScrollbar class is used to add horizontal and vertical scrollbar.
- JtextField: The object of a JtextField class is a text component that allows the editing of a single line text.

So, at the start after running the program it directly opens the "Password Manager",



Then after we click on add option we could add any username and password.



The screenshot shows a web browser window with a light gray background. At the top left, there is a small icon of a document with a flame. The title bar of the window shows standard minimize, maximize, and close buttons. The main content area has the text "ADD ITEM" in bold blue font. Below this, there are three input fields stacked vertically. The first is labeled "Name:" and has a blue border. The second is labeled "Username:" and has a white border. The third is labeled "Password:" and has a white border. In the bottom right corner, there is a green button with the text "Submit" in white.

And in the Add item section we can see edit area. And next we can enter and save our credentials in the add item page, it will be automatically get saved in the all-items list (Arrays) after clicking on the add button. So, in this way we can save all our important credentials in our manager

When we click on submit the data gets stored in back end as below

The screenshot shows the phpMyAdmin interface in a web browser. The URL is localhost/phpmyadmin/index.php?route=/sql&db=miniproject&table=miniproject&pos=0. The interface displays the 'miniproject' table with 7 rows. The table has columns 'name', 'Username', and 'password'. The data is as follows:

name	Username	password
Advait	Advait	Advait123
hgg	khvjkgjb	lji
gvhvm	kjgkmgj	fhggh
Atharva	Atharva@gmail.com	fhgghatharva4356
adv	adva234	g877tyyu
atharva	atharva12	dtcf334
atharv	fhgd	24tgfty

The interface also shows a SQL query editor with the query 'SELECT * FROM `miniproject`' and various toolbars for database management and query execution.

Learning Outcome

We studied about the graphics interface, how to add a database , studied concept of JAVA UI.