Industrial Internship Report on

Password Manager

Prepared by

Vidhi Bhutia

Executive Summary
This report provides details of the Industrial Internship provided by upskill Campus and The IoT Academy in collaboration with Industrial Partner UniConverge Technologies Pvt Ltd (UCT). This internship was focused on a project/problem statement provided by UCT. We had to finish the project including the report in 6 weeks' time. My project was password manager. This internship gave me a very good opportunity to get exposure to Industrial problems and design/implement solution for that. It was an overall great experience to have this internship.

1. Preface

This report documents the development and functionality of a Personal Password Manager application. The application is designed to help users securely store and manage their passwords for various websites and online platforms.

2. Introduction

2.1. About UniConverge Technologies Pvt Ltd

UniConverge Technologies Pvt Ltd is a leading software development company specializing in creating innovative solutions for personal and enterprise needs. The Personal Password Manager application is one of the initiatives aimed at enhancing digital security and convenience for users.

2.2. About upskill Campus

The upskill Campus platform serves as a learning and development hub for employees of UniConverge Technologies Pvt Ltd. It provides resources and training materials to help employees enhance their skills and knowledge in various domains, including software development and cybersecurity.

2.3. Objective

The objective of the Personal Password Manager application is to provide users with a secure and user-friendly solution for storing and managing their

passwords. The application aims to simplify the process of password management while ensuring the highest standards of security.

2.4. Glossary

- Tkinter: Tkinter is the standard GUI (Graphical User Interface) toolkit for Python.

- PIL: PIL (Python Imaging Library) is a library for adding image processing capabilities to Python interpreters.

3. Problem Statement

Users often struggle to remember multiple passwords for various websites and online services. Moreover, storing passwords insecurely, such as in plain text files or spreadsheets, poses significant security risks. The Personal Password Manager application addresses these challenges by providing a secure and convenient way to store and manage passwords.

4. Existing and Proposed Solution

Existing solutions for password management include built-in browser password managers and third-party password management applications. However, these solutions may lack certain features or may not meet users' specific requirements. The proposed solution offers a customizable and user-friendly interface for managing passwords efficiently.

5. Proposed Design/ Model

5.1. High-Level Diagram (if applicable)

The application follows a simple yet effective design, allowing users to add, remove, edit, and view passwords through a graphical user interface.

5.2. Low-Level Diagram (if applicable)

No low-level diagram is provided in the code.

5.3. Interfaces (if applicable)

The application interface is built using the Tkinter library in Python, providing users with intuitive buttons and dialog boxes for interacting with the password management functionalities.

6. Performance Test

6.1. Test Plan/ Test Cases

The performance testing primarily focuses on the responsiveness and reliability of the application under various usage scenarios.

6.2. Test Procedure

Test procedures involve simulating user interactions, including adding, removing, editing, and viewing passwords, to assess the application's performance.

6.3. Performance Outcome

The performance outcome should indicate that the application functions smoothly without significant lag or errors during typical usage.

7. My Learnings

Developing the Personal Password Manager application has provided valuable insights into GUI programming with Tkinter, file I/O operations in Python, and the importance of secure password management practices.

8. Future Work Scope

Future enhancements for the application may include implementing additional security features such as encryption for stored passwords, support for generating strong passwords, and integration with cloud storage services for backup and synchronization.

GitHub: https://github.com/Vidhi-bhutia/UpskillCampus/