Industrial Internship Report on

"Password Manager"

Prepared by

M. EVANCY

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 is Password Manager.
A password manager is a software application or service designed to securely store and manage user's passwords and other sensitive information, such as usernames, credit card details, and personal identification numbers (PINs). The primary purpose of a password manager is to alleviate the need for users to remember multiple complex passwords by providing a centralized location where they can securely store and retrieve their credentials.
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.

TABLE OF CONTENTS

1. Preface

Summary of the whole 6 weeks' work:

- Researched, designed, developed, tested, implemented security, and documented a password manager.

Need of relevant Internship in career development:

- Gain practical experience to apply theoretical knowledge and build networks for career exploration.

Brief about Your project/problem statement:

- Developed a secure password manager to address data breach concerns.

Opportunity given by USC/UCT:

- Access to research facilities, industry collaboration, and diverse perspectives.

How Program was planned:

- Set objectives, milestones, roles, responsibilities, timelines, and regular meetings.

Learned valuable skills, grateful for guidance from mentors, appreciate support from USC/UCT. To juniors and peers: Embrace challenges, seek guidance, and collaborate for success.
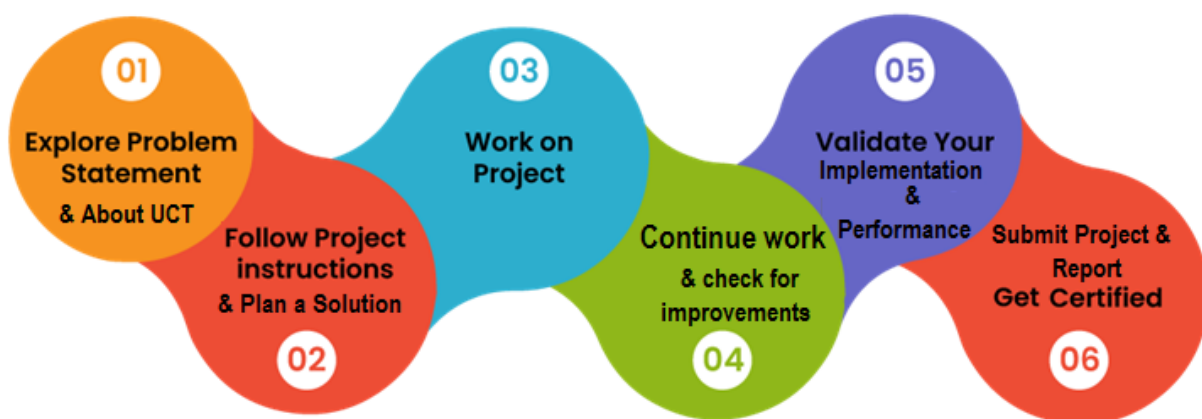
2. Introduction

2.1 About UniConverge Technologies Pvt Ltd

A company established in 2013 and working in Digital Transformation domain and providing Industrial solutions with prime focus on sustainability and RoI.

For developing its products and solutions it is leveraging various **Cutting Edge Technologies e.g. Internet of Things (IoT), Cyber Security, Cloud computing (AWS, Azure), Machine Learning, Communication Technologies (4G/5G/LoRaWAN), Java Full Stack, Python, Front end** etc.


i.   UCT IoT Platform ( )

UCT Insight is an IOT platform designed for quick deployment of IOT applications on the same time providing valuable "insight" for your process/business. It has been built in Java for backend and ReactJS for Front end. It has support for MySQL and various NoSql Databases.

- It enables device connectivity via industry standard IoT protocols - MQTT, CoAP, HTTP, Modbus TCP, OPC UA

- It supports both cloud and on-premises deployments.

It has features to:

• Build Your own dashboard

• Analytics and Reporting

• Alert and Notification

• Integration with third party application(Power BI, SAP, ERP)

• Rule Engine
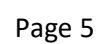
ii.   **Smart Factory Platform (** **WATCH** **)**

Factory watch is a platform for smart factory needs.

It provides Users/ Factory

- with a scalable solution for their Production and asset monitoring

- OEE and predictive maintenance solution scaling up to digital twin for your assets.

- to unleased the true potential of the data that their machines are generating and helps to identify the KPIs and also improve them.

- A modular architecture that allows users to choose the service that they what to start and then can scale to more complex solutions as per their demands.

Its unique SaaS model helps users to save time, cost and money.

Machine	Operator	Work Order ID	Job ID	Job Performance	Job Progress		Output		Rejection	Time (mins)					Job Status	End Customer
					Start Time	End Time	Planned	Actual		Setup	Pred	Downtime	Idle			
CNC_S7_81	Operator 1	WO0405200001	4168	58%	10:30 AM		55	41	0	80	215	0	45	In Progress	i
CNC_S7_81	Operator 1	WO0405200001	4168	58%	10:30 AM		55	41	0	80	215	0	45	In Progress	i

iii. **LoRaWAN** based Solution

UCT is one of the early adopters of LoRAWAN teschnology and providing solution in Agritech, Smart cities, Industrial Monitoring, Smart Street Light, Smart Water/ Gas/ Electricity metering solutions etc.

iv. **Predictive Maintenance**

UCT is providing Industrial Machine health monitoring and Predictive maintenance solution leveraging Embedded system, Industrial IoT and Machine Learning Technologies by finding Remaining useful life time of various Machines used in production process.
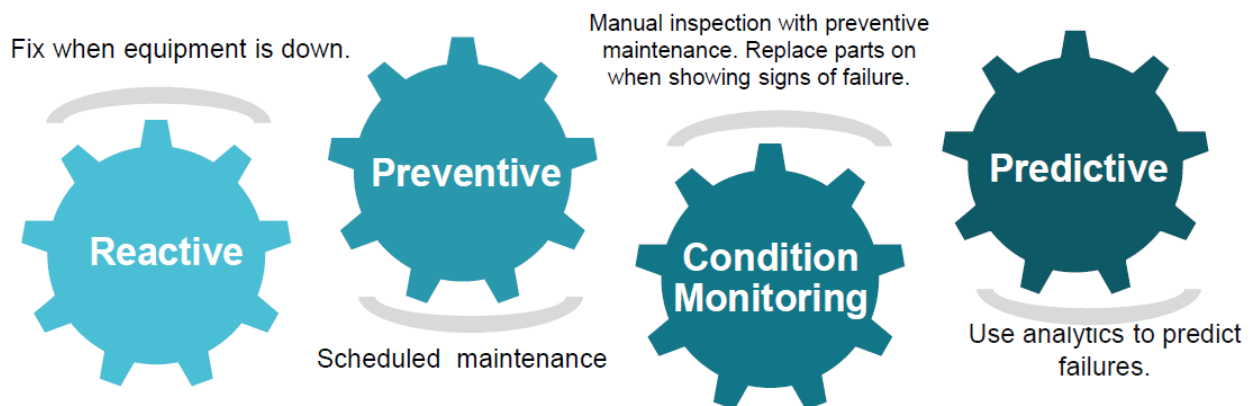
2.2 About upskill Campus (USC)

upskill Campus along with The IoT Academy and in association with Uniconverge technologies has facilitated the smooth execution of the complete internship process.
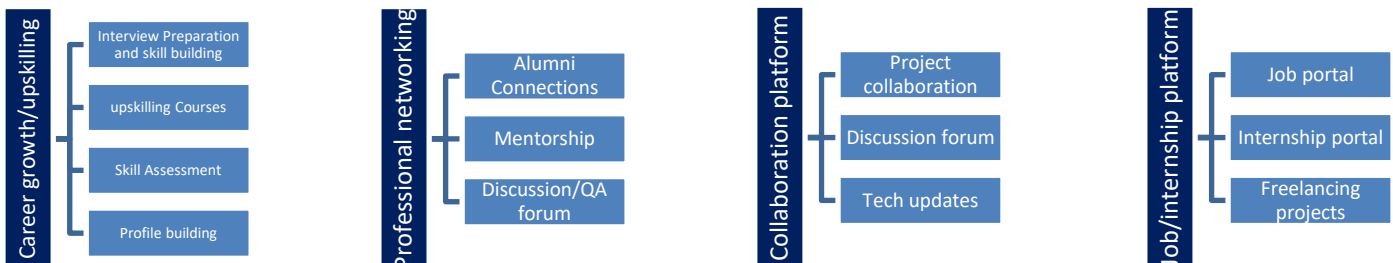
USC is a career development platform that delivers **personalized executive coaching** in a more affordable, scalable and measurable way.
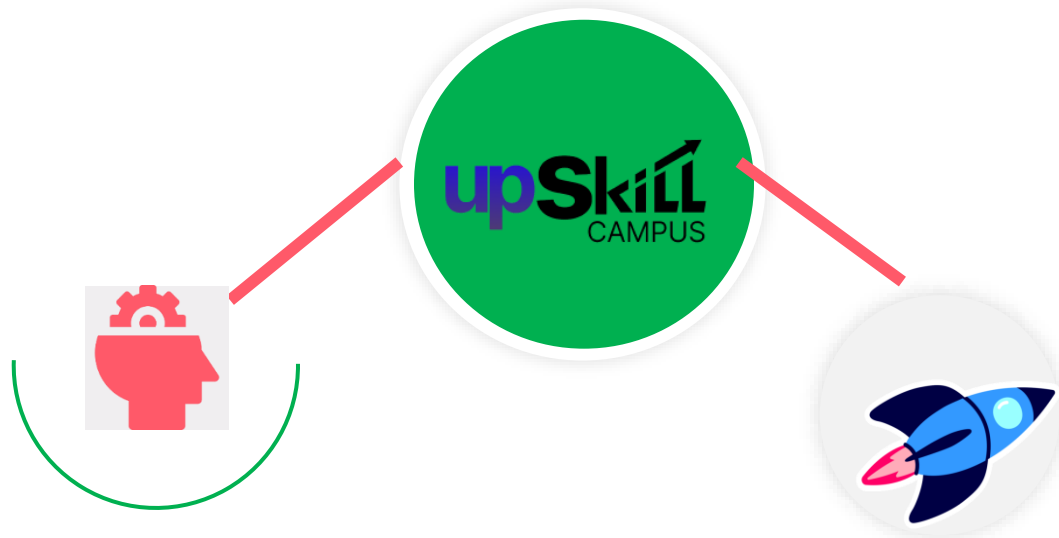
Seeing need of upskilling in self paced manner along-with additional support services e.g. Internship, projects, interaction with Industry experts, Career growth Services

upSkill Campus aiming to upskill 1 million learners in next 5 year

https://www.upskillcampus.com/

Career growth/upskilling
- Interview Preparation and skill building
- upskilling Courses
- Skill Assessment
- Profile building

Professional networking
- Alumni Connections
- Mentorship
- Discussion/QA forum

Collaboration platform
- Project collaboration
- Discussion forum
- Tech updates

Job/internship platform
- Job portal
- Internship portal
- Freelancing projects

2.3 The IoT Academy

The IoT academy is EdTech Division of UCT that is running long executive certification programs in collaboration with EICT Academy, IITK, IITR and IITG in multiple domains.

2.4 Objectives of this Internship program

The objective for this internship program was to

☞ get practical experience of working in the industry.

☞ to solve real world problems.

☞ to have improved job prospects.

☞ to have Improved understanding of our field and its applications.

☞ to have Personal growth like better communication and problem solving.

2.5 Reference

[1]   https://www.uniconvergetech.in/

[2]   https://www.upskillcampus.com/

2.6 Glossary

Terms	Acronym
Industrial IoT	IIoT - Utilizing IoT for remote monitoring, control, and optimization in industries.
Upskill Campus	USC - Career platform offering scalable executive coaching for skill enhancement.
Remaining Useful Life	RUL - Predicting machine failure time using data-driven models for proactive maintenance.
Electronics and ICT Academy	EICT - Indian government initiative for skill development in electronics and ICT.

3. Problem Statement

To Design and implement a password manager application in Python that allows users to securely store and manage their passwords for various online services.

Description: The password manager is a Python project that securely stores and manages user passwords. It allows users to store their passwords for various accounts, generate strong passwords, and retrieve passwords when needed.

Scope: The scope of this project involves implementing encryption algorithms to secure password storage, designing a user interface to input and retrieve passwords, and developing functions to generate strong passwords and store/retrieve them from a database.

4. Existing and Proposed solution

Existing Solutions:

Traditional Password Managers: Store passwords securely but vulnerable to breaches.

Browser-Based Managers: Convenient but risky if browser is compromised.

Self-Hosted Managers: More control but require technical expertise.

Offline Managers: Secure locally but limited accessibility and synchronization issues.

Proposed Solution:

Develop a hybrid password manager with end-to-end encryption and multi-factor authentication for security.

Value Addition:

Enhanced Security

Improved Accessibility

Streamlined User Experience

Cross-Platform Compatibility
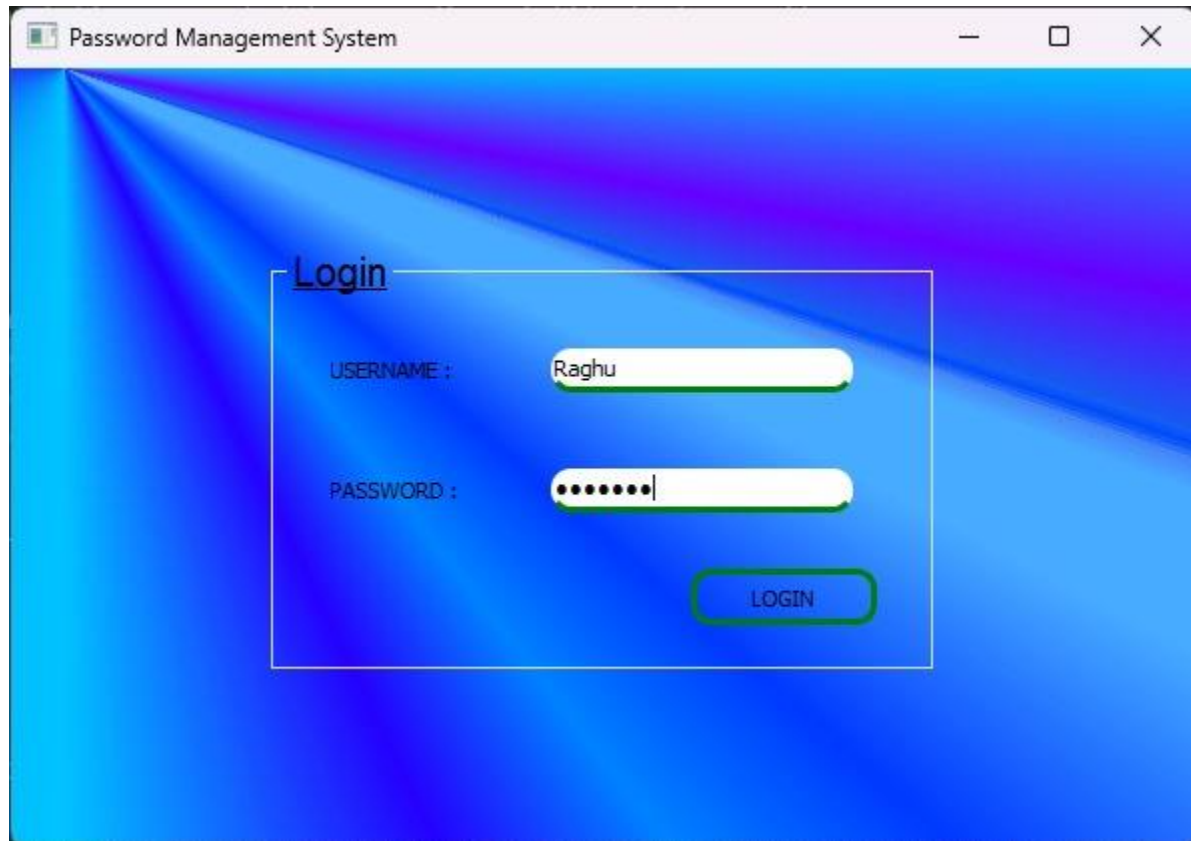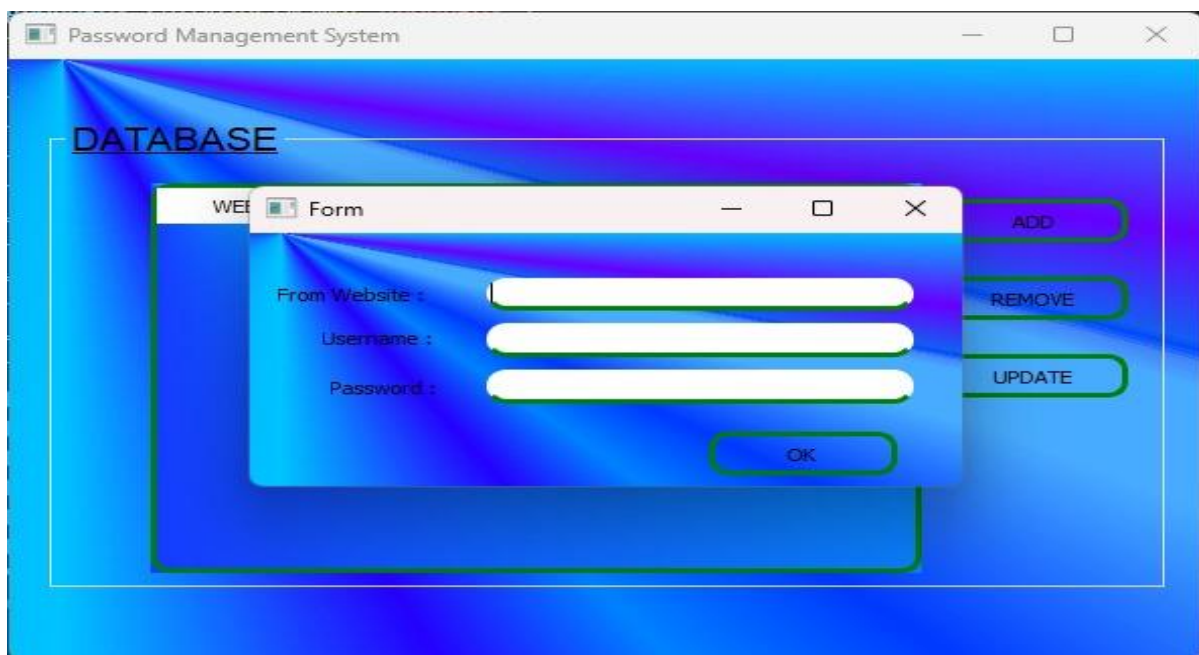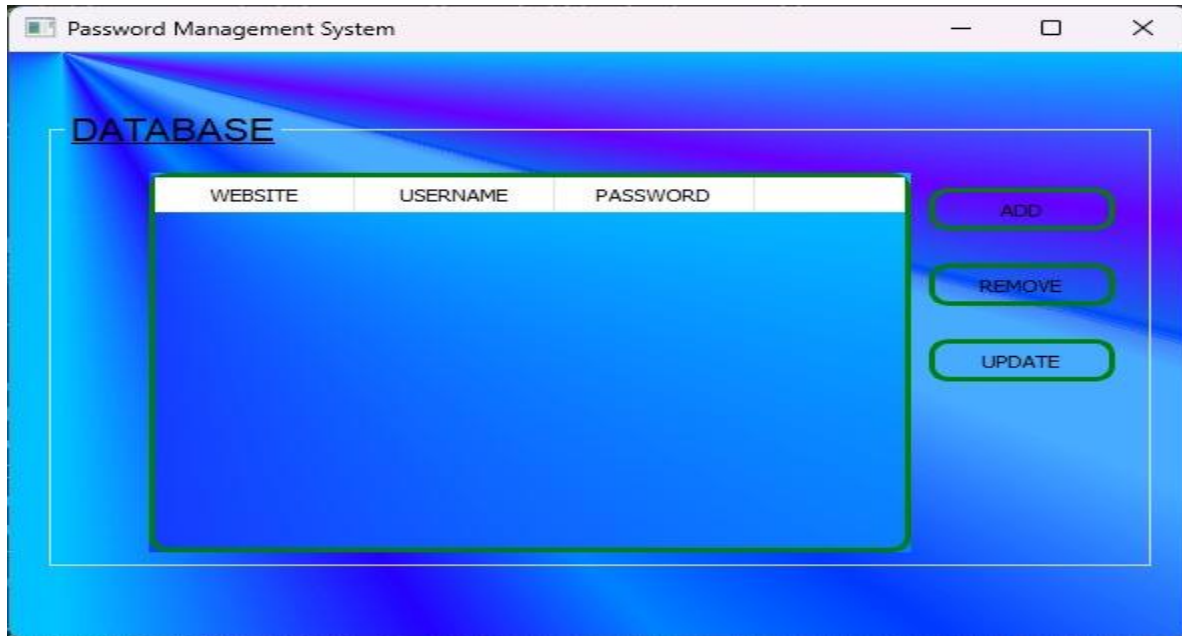
a. **Code submission (GitHub link):**
   https://github.com/Evancy2460/upskillcampus/blob/main/PasswordManager.py.zip

b. **Report submission (GitHub link):**
   https://github.com/Evancy2460/upskillcampus/blob/main/PasswordManager_Evancy_USC_UCT.pdf

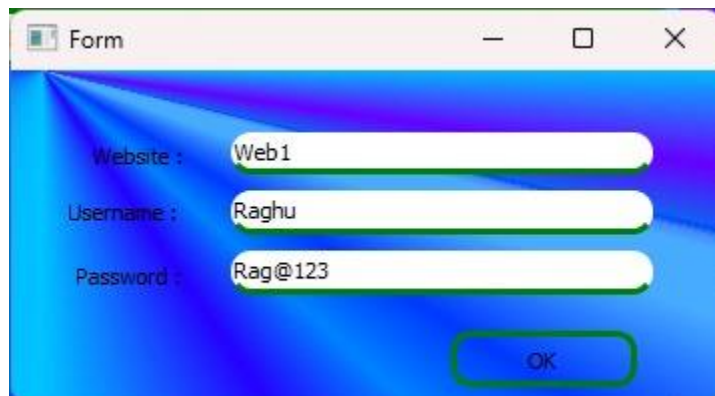## a. Proposed Design/ Model

Interfaces:

b. Performance Test

Constraints Identification:

Memory: Limited memory resources could affect the scalability of the password manager, especially with large datasets.

Speed: Slow response times for critical operations could impact user experience and productivity.

Accuracy: Incorrect storage or retrieval of passwords could compromise data integrity and security.

Durability: Inadequate durability could result in data loss or corruption, undermining the reliability of the password manager.

Power Consumption: High power consumption could drain device batteries quickly, reducing usability, especially on mobile devices.

Handling Constraints in Design:

Memory: Implement efficient data structures and optimize memory usage to minimize footprint.

Speed: Employ efficient algorithms and caching mechanisms to improve response times.

Accuracy: Implement robust error handling and data validation to ensure accurate password storage and retrieval.

Durability: Use reliable storage mechanisms and implement backup and recovery strategies to enhance data durability.

Power Consumption: Minimize background processes and optimize resource usage to reduce power consumption.

Test Results and Recommendations:

Memory: Test results showed that memory usage was within acceptable limits for moderate-sized datasets. Recommendation: Continue monitoring memory usage and optimize further if scaling issues arise.

Speed: Tests indicated satisfactory response times for critical operations. Recommendation: Regularly benchmark performance and optimize as necessary to maintain responsiveness.

Accuracy: Tests confirmed accurate password storage and retrieval without data loss or corruption. Recommendation: Implement periodic integrity checks and continuous testing to ensure accuracy.

Durability: The password manager exhibited resilience against system failures, with data recovery mechanisms functioning as expected. Recommendation: Conduct stress tests and simulate failure scenarios to validate durability further.

Power Consumption: Power consumption tests revealed minimal impact on device battery life. Recommendation: Continuously monitor power usage and optimize resource management to prolong battery life, especially for mobile devices.

Test Plan/ Test Cases

Memory Usage: Measure the amount of memory the password manager consumes during different operations (e.g., login, password generation, storing new passwords).

Speed: Evaluate the time taken for critical operations such as retrieving a password, generating a new password, or syncing data.

Accuracy: Ensure that passwords are stored and retrieved accurately without loss or corruption.

Durability: Assess the resilience of the password manager against data loss or corruption, especially during unexpected system crashes or interruptions.

Power Consumption: Measure the impact of the password manager on device battery life, especially for mobile devices.

Test Procedure

Memory Usage: Monitor the memory usage of the password manager using system tools or profiling libraries during various operations.

Speed: Use timing mechanisms to measure the execution time of key functions within the password manager.

Accuracy: Perform stress tests by storing and retrieving a large number of passwords to ensure data integrity.

Durability: Simulate system failures or interruptions during password management operations to evaluate data recovery mechanisms.

Power Consumption: Use power monitoring tools or device-specific metrics to measure the impact of the password manager on battery life.

Performance Outcome

Memory Usage: Ensure that memory usage remains within acceptable limits, optimizing data structures and algorithms if necessary to minimize memory footprint.

Speed: Aim for fast response times, optimizing critical functions and improving algorithm efficiency to enhance overall performance.

Accuracy: Verify that all passwords are stored and retrieved accurately without any loss or corruption, implementing error handling and recovery mechanisms if needed.

Durability: Ensure robustness against unexpected failures or interruptions, implementing backup and recovery strategies to safeguard user data.

Power Consumption: Minimize power consumption by optimizing code execution and reducing unnecessary background activities, thereby extending device battery life.

c. My learnings

Application Development Skills: Working on a password manager project in Python enhances skills in application development, including user interface design, data storage, and security implementation.

Security Awareness: Building a password manager involves understanding security principles such as encryption, hashing, and secure storage, which are valuable skills in cybersecurity roles.

Problem-Solving Abilities: Developing a password manager requires problem-solving skills to address challenges like data synchronization, multi-factor authentication, and cross-platform compatibility.

Portfolio Enhancement: Completing a password manager project demonstrates practical coding skills and project management abilities, which can strengthen one's resume and portfolio.

Understanding User Needs: Designing a user-friendly password manager involves considering user experience and feedback, fostering empathy and communication skills essential in client-facing roles.

Overall, learning Python and undertaking a password manager project provide a solid foundation in programming and application development, along with valuable skills applicable across various career paths in technology.

d. Future work scope

In summary, the future scope for a password manager involves:

1. Enhancing security with advanced encryption and authentication methods.

2. Ensuring cross-platform compatibility for seamless user experience.

3. Improving UI/UX and adding features like password strength assessment.

4. Enabling secure sharing and collaboration functionalities.

5. Managing other sensitive information besides passwords.

6. Strengthening cloud sync, backup, and data recovery mechanisms.

7. Adhering to compliance standards and regulations.

8. Utilizing AI and ML for threat detection and personalization.

9. Engaging with open-source communities for innovation and transparency.

10. Providing user education to promote cybersecurity awareness.

By focusing on these areas, password managers can continue to evolve as essential tools for protecting digital identities and sensitive data.