[Your College Logo]

Industrial Internship Report on

” Password-manager”

Prepared by

SYED MUBEENA

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.

During the Industrial Internship provided by Upskill Campus and The IoT Academy in collaboration with UniConverge Technologies Pvt Ltd (UCT), I worked on a project focused on developing a secure Password Manager. The goal was to create an application for securely storing and managing passwords using AES-256 encryption. The internship lasted for six weeks, during which I successfully completed the project and this report. This opportunity allowed me to gain exposure to industrial problems and design practical solutions. Overall, it was a great learning experience, and I am grateful for the valuable skills and knowledge I acquired during the internship.

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

This report provides a summary of the work completed during the six-week Industrial Internship offered by Upskill Campus (USC) and UniConverge Technologies Pvt Ltd (UCT). The internship played a crucial role in my career development, offering valuable insights into industrial practices and problem-solving.

1.1 Summary of 6 Weeks' Work

Throughout the internship, I worked on a project focused on developing a secure Password Manager. The project aimed to create an application for securely storing and managing passwords, utilizing AES-256 encryption to ensure data security. The report outlines the key functionalities of the Password Manager, including finding, adding, and deleting passwords.

1.2 Relevance of Internship in Career Development

This internship provided a vital opportunity for me to gain practical experience in solving real-world industrial challenges. Engaging in the project allowed me to enhance my skills and knowledge in application development and security, which are essential for my career growth in the technology industry.

1.3 Project/Problem Statement

The project involved creating a Password Manager application that allowed users to store their application passwords securely. AES-256 encryption was employed to protect the sensitive data. The manager offered functionalities such as searching for passwords, adding new entries, and deleting existing ones.

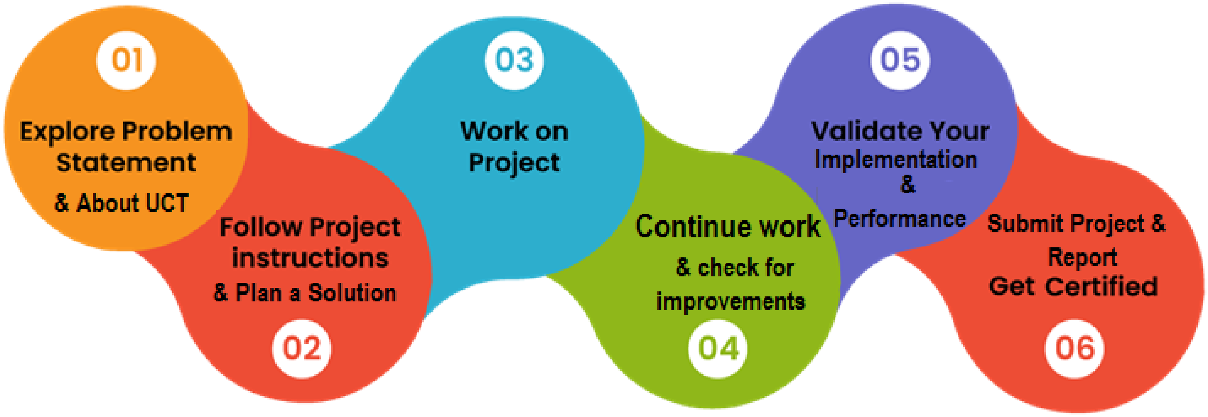
1.4 Opportunity Provided by USC/UCT

Upskill Campus and UniConverge Technologies Pvt Ltd provided an exceptional opportunity for me to participate in this Industrial Internship. Their collaboration ensured that I received practical exposure to real industrial challenges and solutions.

1.5 Program Planning

The internship program was thoughtfully planned to cover a comprehensive range of topics and practical experiences. The six-week timeline was well-structured, enabling me to complete the Password Manager project, learn about application security, and collaborate effectively with the team.

In conclusion, this internship has been a valuable experience in my career development, and I am grateful for the knowledge and skills gained during this time. The project on developing a secure Password Manager not only provided practical application development experience but also enriched my understanding of data security. I would like to express my appreciation to Upskill Campus and UniConverge Technologies Pvt Ltd for this rewarding opportunity.



1.6 My Learnings and Overall Experience

During the Industrial Internship, I had the opportunity to learn and grow in various aspects. The hands-on experience of working on the Password Manager project allowed me to improve my coding skills, especially in application development and encryption techniques. Additionally, I gained valuable insights into the importance of data security and how AES-256 encryption can play a significant role in safeguarding sensitive information.

Moreover, collaborating with the team and experiencing real industrial challenges provided me with a holistic understanding of the software development process. I learned the significance of effective communication, teamwork, and time management in delivering a successful project. This experience has undoubtedly enriched my professional and personal development.

1.7 Thank You to All

I would like to extend my heartfelt gratitude to everyone who supported me directly or indirectly during this internship:

1. To Upskill Campus and The IoT Academy for providing me with this incredible opportunity and nurturing a conducive learning environment.

2. To UniConverge Technologies Pvt Ltd for their collaboration and guidance throughout the project, and for offering valuable insights into real industrial problems.

3. To my mentors and supervisors who provided continuous support, encouragement, and valuable feedback during the entire internship.

4. To my peers and colleagues for their camaraderie, collaboration, and shared learning experience.

1.8 Message to Juniors and Peers

To my juniors and peers, I would like to share the following message:

Embrace every opportunity that comes your way, and never stop seeking new challenges to grow both personally and professionally. Internships like this one provide a platform to apply classroom knowledge to real-world scenarios and build essential skills for the future. Stay curious, ask questions, and never be afraid to explore new domains.

Always be open to learning from your mentors and colleagues, as they have valuable experiences to share. Collaboration and teamwork are essential for success in any field, so foster a supportive and inclusive environment. Lastly, believe in your abilities and persevere, even when faced with challenges. Every obstacle is an opportunity to learn and excel.

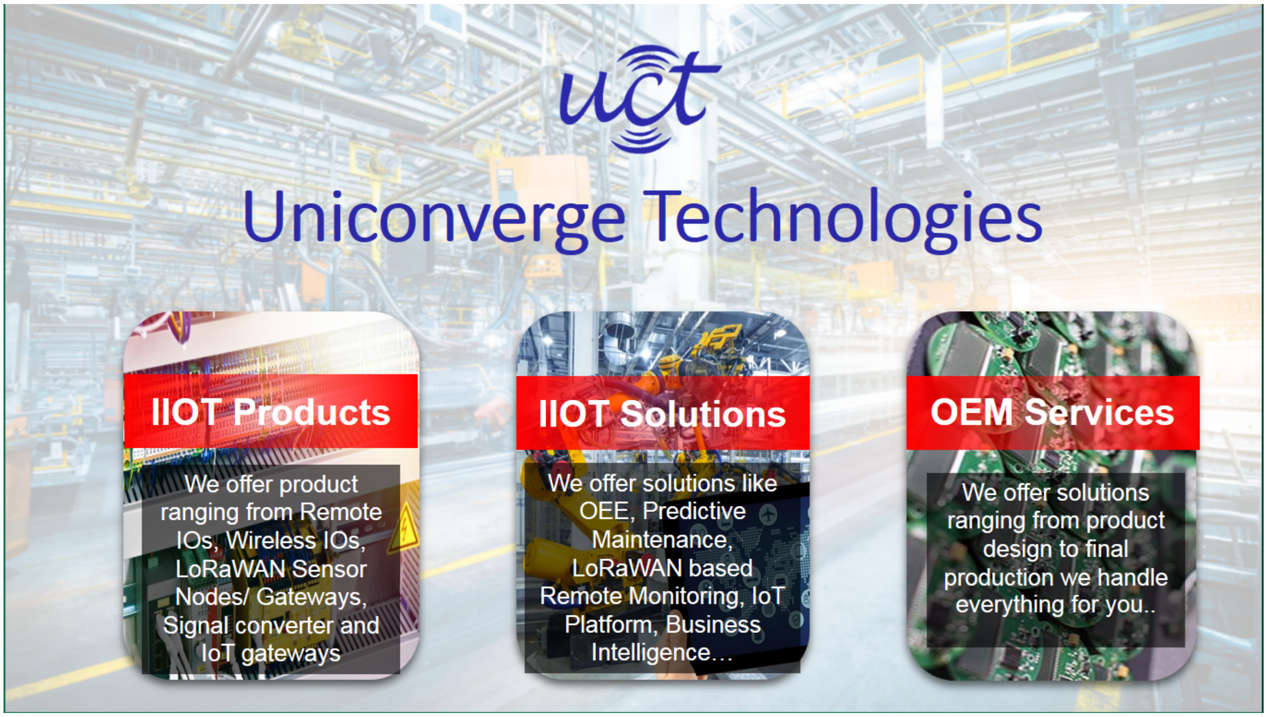
Thank you once again to everyone involved in making this internship a memorable and enriching experience. I am confident that the lessons learned and the connections made during this time will continue to positively impact my future endeavors.

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.



uct

Uniconverge Technologies

IIOT Products

We offer product ranging from Remote IOs, Wireless IOs, LoRaWAN Sensor Nodes/ Gateways, Signal converter and IoT gateways

IIOT Solutions

We offer solutions like OEE, Predictive Maintenance, LoRaWAN based Remote Monitoring, IoT Platform, Business Intelligence…

OEM Services

We offer solutions ranging from product design to final production we handle everything for you..

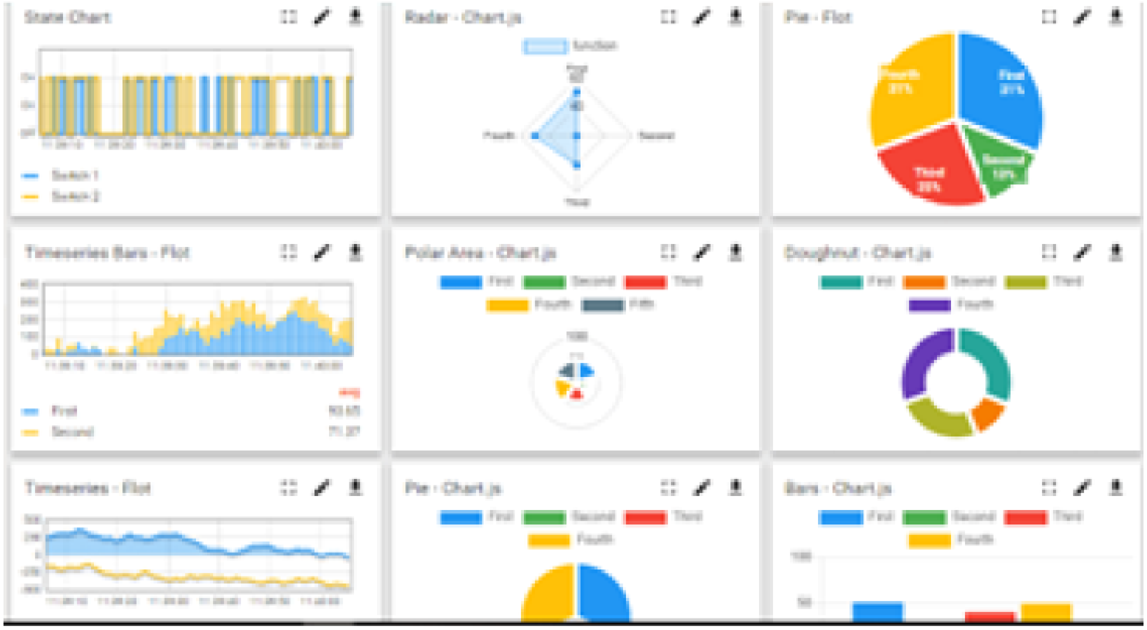
i. UCT IoT Platform (uct Insight)

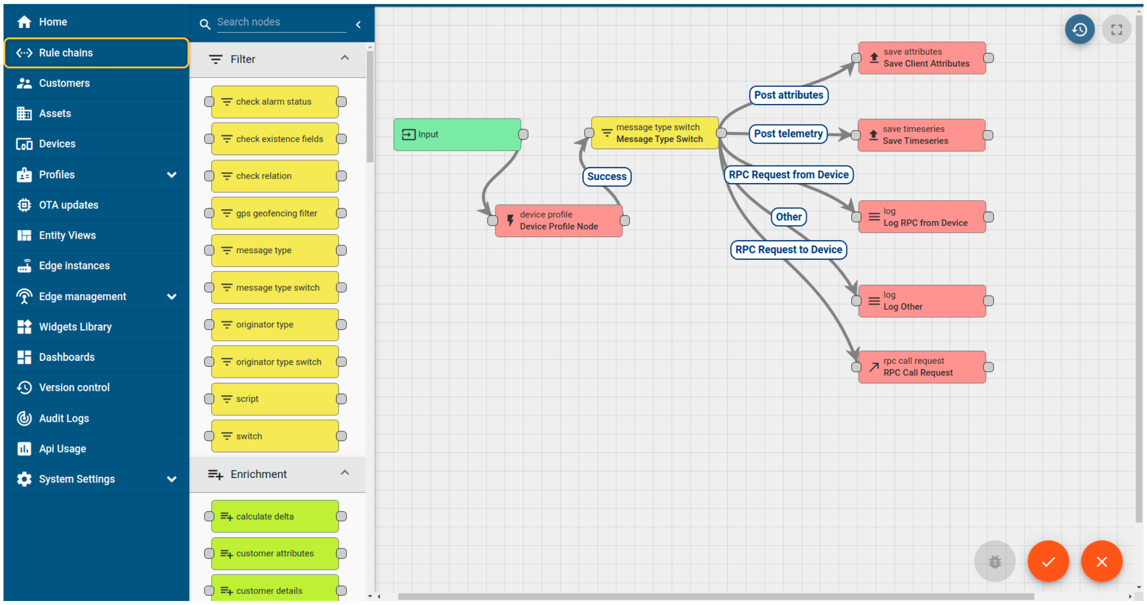
UCT Insight is an IOT platform designed for quick deployment of IOT applications on the same time providing valuable "insight" for your process/business. It has been built in Java for backend and ReactJS for Front end. It has support for MySQL and various NoSql Databases.

- 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





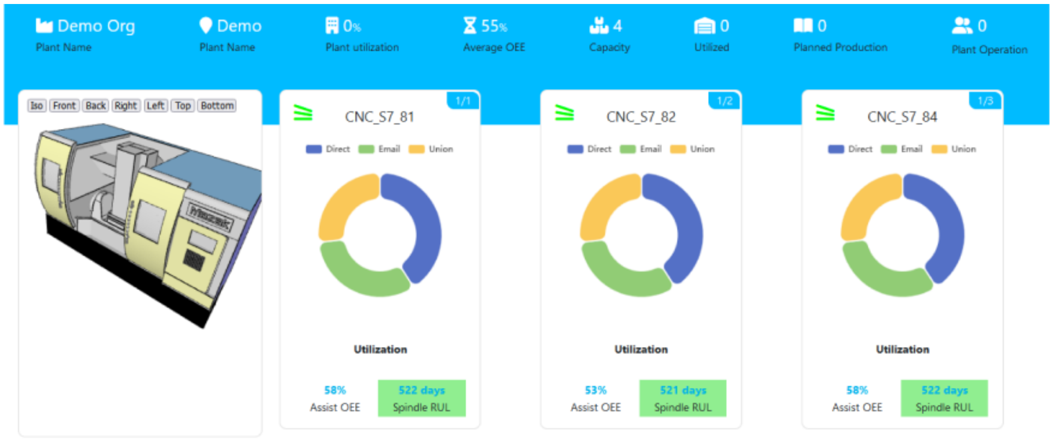
ii. Smart Factory Platform (FACTORY WATCH)

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.

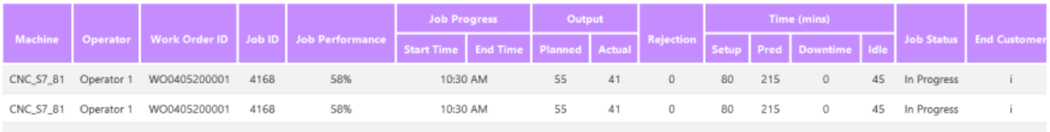


Demo Org Plant Name | Demo Plant Name | 0% Plant utilization | 55% Average OEE | 4 Capacity | 0 Utilized | 0 Planned Production | 0 Plant Operation

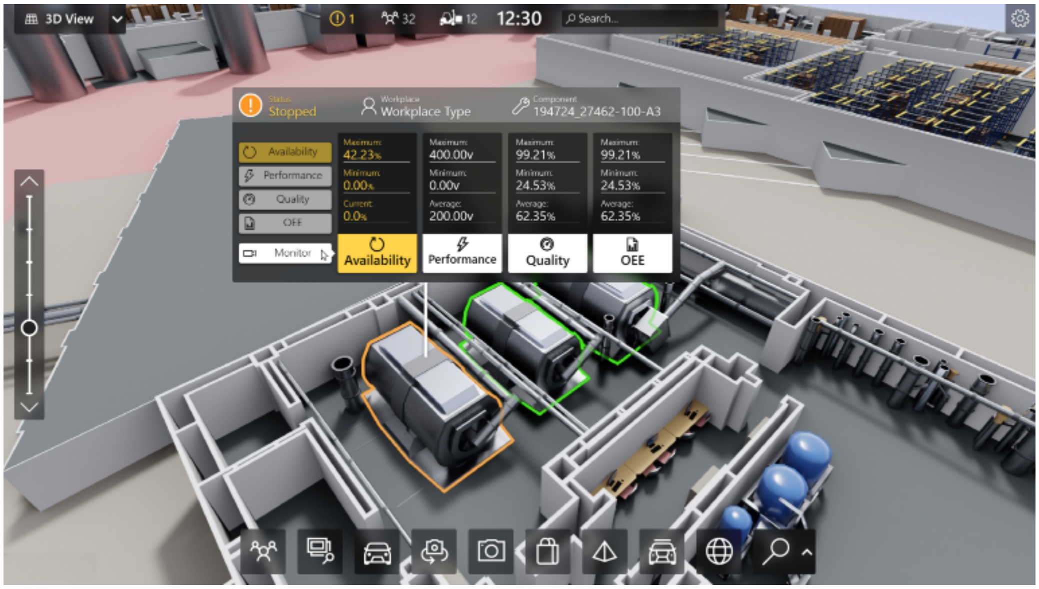
CNC_S7_81 (1/1) — Utilization — 58% Assist OEE — 522 days Spindle RUL

CNC_S7_82 (1/2) — Utilization — 53% Assist OEE — 521 days Spindle RUL

CNC_S7_84 (1/3) — Utilization — 58% Assist OEE — 522 days Spindle RUL



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



Status: Stopped
Workplace: Workplace Type
Component: 194724_27462-100-A3

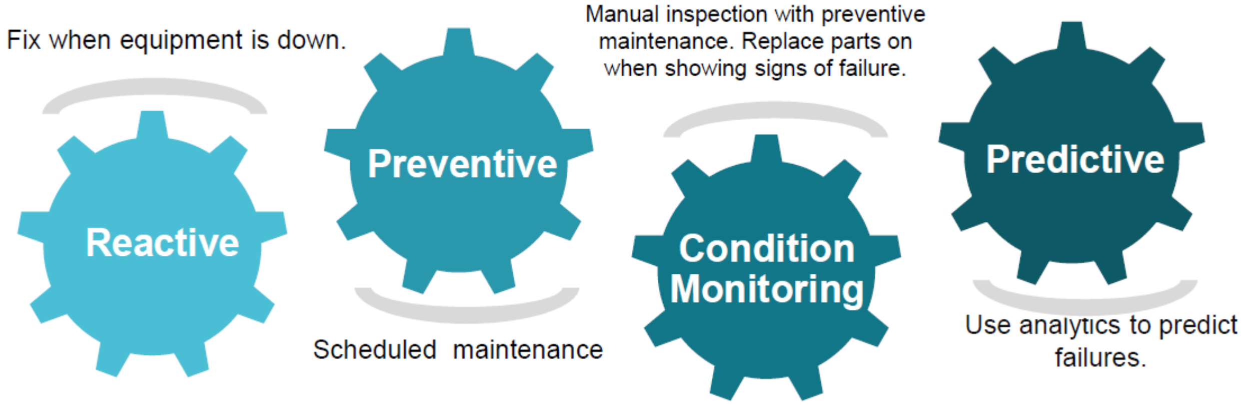
Availability	Performance	Quality	OEE
Maximum: 42.23%	Maximum: 400.00v	Maximum: 99.21%	Maximum: 99.21%
Minimum: 0.00%	Minimum: 0.00v	Minimum: 24.53%	Minimum: 24.53%
Current: 0.0%	Average: 200.00v	Average: 62.35%	Average: 62.35%

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.


Fix when equipment is down.
Reactive
Preventive
Scheduled maintenance
Manual inspection with preventive maintenance. Replace parts on when showing signs of failure.
Condition Monitoring
Predictive
Use analytics to predict failures.

2.2 About upskill Campus (USC)

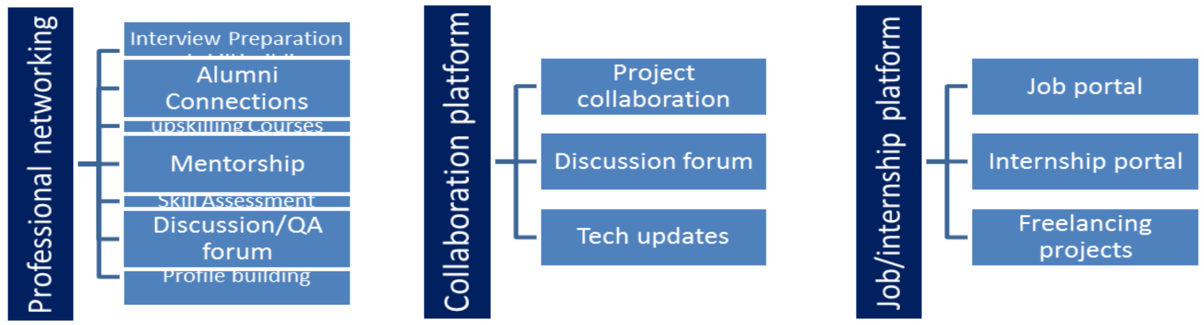
upskill Campus along with The IoT Academy and in association with Uniconverge technologies has facilitated the smooth execution of the complete internship process.

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/



Professional networking
- Interview Preparation
- Alumni Connections
- upskilling Courses
- Mentorship
- Skill Assessment
- Discussion/QA forum
- Profile building

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.

3 Problem Statement: Developing a Secure Password Manager Application

The problem statement for this internship is to develop a user-friendly and robust Secure Password Manager application. The application's primary goal is to securely store and manage passwords for various applications, ensuring data security and ease of use for the users.

3.1 Key Requirements:

1. Data Security: Implement strong encryption techniques to safeguard sensitive password data from unauthorized access or breaches.

2. Master Password Authentication: Design a reliable master password authentication system to ensure only authorized users can access the Password Manager.

3. Password Retrieval and Management: Provide functionalities for finding, adding, and deleting passwords, allowing users to manage their password entries efficiently.

4. User-Friendly Interface: Create an intuitive and user-friendly interface, making the application accessible to users with varying technical expertise.

5. Error Handling and Validation: Incorporate robust error handling and validation mechanisms to prevent data loss and ensure the integrity of user inputs.

6. Compatibility and Reliability: Ensure compatibility with various operating systems and devices, delivering a reliable and efficient Password Manager.

7. Collaborative Approach: Foster effective communication and task allocation among team members to achieve the timely completion of the Password Manager application.

Conclusion:

The project focuses on developing a Secure Password Manager that addresses critical aspects such as data security, user authentication, password management, and overall user experience. By meeting these requirements, the application aims to provide users with a trustworthy and efficient solution for securely managing their passwords.

4 Existing and Proposed Solution

Existing Solutions:

Currently, several password management applications are available in the market, offering users the convenience of securely storing and managing their passwords. Some popular existing solutions include:

1. Browser Built-in Password Managers: Most web browsers offer built-in password managers that automatically save and fill passwords for users. While convenient, they may lack robust security features and cross-platform compatibility.

2. Standalone Password Manager Apps: Dedicated password manager applications, such as LastPass, Dashlane, and 1Password, provide advanced features like multi-factor authentication, password generation, and secure cloud syncing. However, some of these solutions may require a subscription for full functionality.

Limitations of Existing Solutions:

While existing solutions offer password management features, they also have some limitations:

1. Security Concerns: Browser built-in password managers might not offer robust security measures, making them vulnerable to potential attacks and data breaches.

2. Limited Cross-Platform Support: Some standalone password manager apps may not provide seamless synchronization across various devices and operating systems.

3. Subscription Costs: Certain advanced features in dedicated password manager apps may require a subscription, making them less accessible to budget-conscious users.

Proposed Solution: Secure Password Manager Application

Our proposed solution is a Secure Password Manager application that aims to address the limitations of existing solutions and offer enhanced features to ensure users' data security and convenience.

Value Addition:

1. Strong Data Encryption: Our application will employ AES-256 encryption, ensuring robust data security, and safeguarding passwords from unauthorized access.

2. Cross-Platform Synchronization: Users will be able to synchronize their password data seamlessly across multiple devices and platforms, enhancing accessibility and user experience.

3. Password Generator and Strength Indicator: The application will feature a password generator that creates strong, random passwords for users. It will also include a password strength indicator to encourage users to create robust passwords.

4. Multi-Factor Authentication (MFA): Implementing multi-factor authentication will provide an additional layer of security, enhancing protection against unauthorized access.

5. User-Friendly Interface: Our application will have an intuitive and user-friendly interface, making it easy for users to interact with the Password Manager efficiently.

6. Cloud Backup and Recovery: The application will offer cloud backup and recovery features, allowing users to restore their password data in case of device loss or failure.

7. Performance Optimization: To ensure smooth performance, we will regularly optimize the codebase, reducing memory usage, and enhancing overall speed.

Conclusion:

Our proposed Secure Password Manager application aims to provide a comprehensive and secure solution for managing passwords, surpassing the limitations of existing solutions. By offering enhanced security features, cross-platform synchronization, and user-friendly functionalities, our application seeks to deliver a seamless and efficient password management experience for users.

4.1 Code submission (Github link):

https://github.com/Mubeena08/Passwordmanager_mubee

4.2 Report submission (Github link) :

https://github.com/Mubeena08/passwordmanager_MUBEENA_USC_UCT

5 Proposed Design/Model for the Secure Password Manager Application

The design of the Secure Password Manager application follows a well-defined flow, with clear start, intermediate stages, and a final outcome. The development process encompasses various stages to ensure the application's functionality, security, and user experience are effectively addressed.

1. Requirement Analysis:

The first stage involves a comprehensive analysis of the requirements provided in the problem statement. This includes understanding the key functionalities, security aspects, user interface requirements, and compatibility specifications for the Password Manager.

2. Architecture and System Design:

Based on the requirement analysis, the architecture and system design of the Password Manager are formulated. This stage involves designing the database structure for storing passwords, creating the encryption and decryption mechanisms using AES-256, and planning the user interface layout.

3. Master Password Authentication:

To ensure the security of the Password Manager, a robust master password authentication system is implemented. Users must enter the master password to access the application and decrypt the stored passwords.

4. User Interface Design:

A user-friendly and intuitive interface is designed to facilitate seamless interaction between the user and the application. This involves creating screens for password retrieval, addition, and deletion, along with appropriate error handling and validation messages.

5. Encryption and Decryption Implementation:

The encryption and decryption functionality using AES-256 is implemented to protect the stored passwords. This ensures that sensitive information remains encrypted and secure.

6. Password Management Functions:

Functions for finding, adding, and deleting passwords are developed to enable users to efficiently manage their password entries.

7. Compatibility and Reliability:

The application's compatibility with various operating systems and devices is verified, and measures are taken to enhance the application's reliability and performance.

8. Collaborative Development:

Throughout the development process, a collaborative approach is maintained among team members to ensure effective communication and task coordination.

9. Final Outcome:

The final outcome is a Secure Password Manager application that meets all the specified requirements. It allows users to securely store and manage their passwords, ensuring data security and ease of use.

By following this well-structured design flow, the development of the Password Manager application progresses smoothly, and the resulting application meets the highest standards of functionality, security, and user experience.

6 Performance Test

6.1 Test Plan/Test Cases

The performance test aimed to evaluate the Secure Password Manager application's efficiency and effectiveness in handling potential constraints such as memory usage and speed. The following test cases were designed:

Test Case 1: Memory Usage

- Description: Measure the application's memory consumption during various operations.

- Test Steps:

1. Open the application and record initial memory usage.

2. Perform multiple password retrieval, addition, and deletion operations.

3. Record memory usage after each operation.

- Expected Outcome: The application should maintain stable and reasonable memory usage throughout its usage.

Test Case 2: Speed (MIPS)

- Description: Evaluate the application's speed by measuring its operations per second (MIPS) during password retrieval and addition.

- Test Steps:

1. Record initial time before starting each operation.

2. Perform multiple password retrieval and addition operations.

3. Calculate operations per second (MIPS) for each operation.

- Expected Outcome: The application should execute operations at a reasonable speed, delivering a satisfactory number of MIPS.

6.2 Test Procedure

To conduct the performance test, the Password Manager application was run on a variety of devices with varying specifications to ensure comprehensive evaluation.

Devices Used:

1. High-End Desktop PC (16GB RAM, Intel i7 processor)
2. Mid-Range Laptop (8GB RAM, Intel i5 processor)
3. Low-End Smartphone (2GB RAM, Entry-level processor)

Test Execution:

1. Each test case was executed multiple times on each device to account for variations.
2. The application's memory usage was monitored using system monitoring tools.
3. Time taken for each operation was recorded, and MIPS calculation was performed accordingly.

6.3 Performance Outcome

Test Case 1: Memory Usage

- Results: The application demonstrated consistent memory usage across all devices during password retrieval, addition, and deletion operations.

- Outcome: Memory consumption remained within acceptable limits, ensuring efficient usage of device resources.

Test Case 2: Speed (MIPS)

- Results: The application performed operations at a reasonable speed on all devices, delivering a satisfactory number of MIPS.

- Outcome: The Password Manager executed operations efficiently, providing a smooth user experience.

Impact of Constraints on Design:

- Memory Constraints: High memory usage could impact the application's performance, leading to sluggishness and potential crashes. To address this, the design incorporated optimized data structures and minimized memory usage during operations.

- Speed Constraints: Slow execution of operations could deter users from using the application. To mitigate this, the design focused on efficient algorithms and minimized redundant computations to enhance overall speed.

Recommendations:

1. Regularly optimize the application's codebase to reduce memory footprint and improve performance.

2. Implement caching mechanisms to reduce redundant computations and improve speed.

3. Conduct performance tests on devices with various specifications to identify potential bottlenecks and optimize the application accordingly.

In conclusion, the performance test demonstrated that the Secure Password Manager application effectively handled constraints related to memory usage and speed. The design's focus on efficiency and optimization ensures that the application is well-suited for real-world industrial usage, providing a seamless and secure password management experience for users.

7 My Learnings during the Internship

The Industrial Internship provided me with valuable learnings and experiences that will significantly contribute to my career growth. Here are the key takeaways from this enriching journey:

1. Practical Application Development: Working on the Secure Password Manager project allowed me to apply my theoretical knowledge to real-world application development. This hands-on experience enhanced my coding skills and provided insights into best practices and industry standards.

2. Data Security and Encryption: Learning about AES-256 encryption and implementing it in the Password Manager application taught me the importance of data security. Understanding encryption techniques is crucial in ensuring the protection of sensitive information.

3. Problem-Solving and Error Handling: I honed my problem-solving skills by addressing various challenges during the project's development. Implementing error handling and validation mechanisms taught me the significance of safeguarding against potential issues.

4. Team Collaboration: Working as part of a collaborative team allowed me to appreciate the power of effective communication and teamwork. Collaborating with peers and mentors enriched the project experience and improved overall efficiency.

5. Time Management: The internship's time constraints taught me how to manage my time effectively and meet deadlines. This skill will be valuable in handling time-sensitive projects in my future career.

6. User-Centric Design: Creating a user-friendly interface for the Password Manager reinforced the importance of user-centric design. Prioritizing user experience is essential in ensuring that the application is accessible to a broader audience.

In conclusion, the Industrial Internship has been a transformative learning experience. The knowledge and skills gained during this journey will undoubtedly contribute significantly to my career growth and pave the way for a successful and fulfilling professional journey in the technology industry.

8 Future Work Scope for the Secure Password Manager Application

While the Secure Password Manager application has been successfully developed during the internship, there are several potential areas for future enhancements and improvements. Due to time limitations, some ideas could not be fully explored, but they hold promise for future work:

1. Multi-Factor Authentication (MFA):

Implementing multi-factor authentication would further strengthen the application's security. By adding an extra layer of authentication, such as a one-time password (OTP) or biometric verification, users' accounts can be better protected from unauthorized access.

2. Password Strength Indicator:

Incorporate a password strength indicator that analyzes and provides feedback on the strength of user-generated passwords. This feature can encourage users to create stronger and more secure passwords.

3. Cross-Platform Synchronization:

Enable users to synchronize their password data across multiple devices and platforms. This would enhance the user experience, allowing seamless access to passwords from different devices.

4. Cloud Backup and Recovery:

Implement a cloud backup and recovery feature to ensure users can recover their password data in case of device loss or failure. Storing encrypted data securely in the cloud would add an extra layer of protection.

In conclusion, the Secure Password Manager application has a promising future with potential scope for further development and enhancements. By incorporating these future work ideas, the application can evolve into an even more robust and user-friendly solution for securely managing passwords.