Industrial Internship Report on

”Password Manager”

Prepared by

[Ludhiya Donthula]

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: 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. 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.

ABLE OF CONTENTS

1 Preface

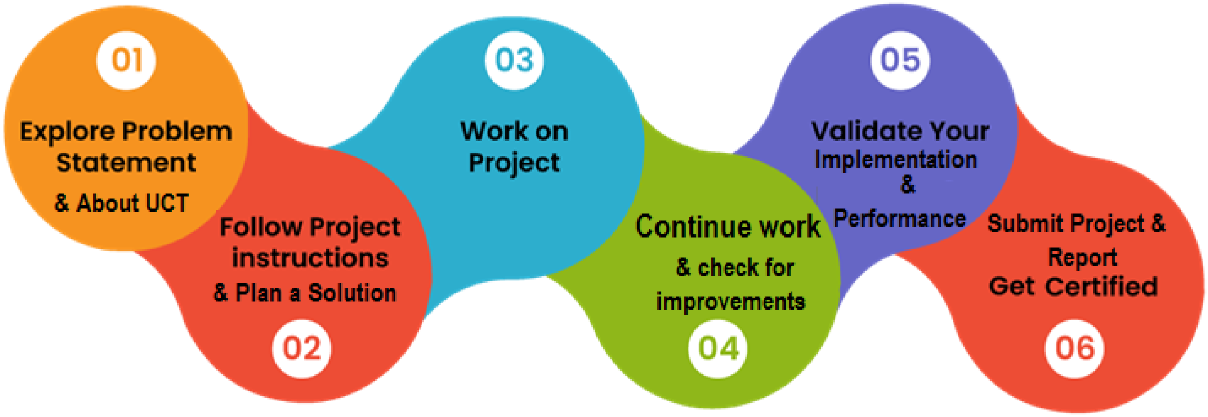
Summary of the whole 6 weeks' work.

About need of relevant Internship in career development.

Brief about Your project/problem statement.

Opportunity given by USC/UCT.

How Program was planned



Your Learnings and overall experience.

Thank to all (with names), who have helped you directly or indirectly.

Your message to your juniors and peers.

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)

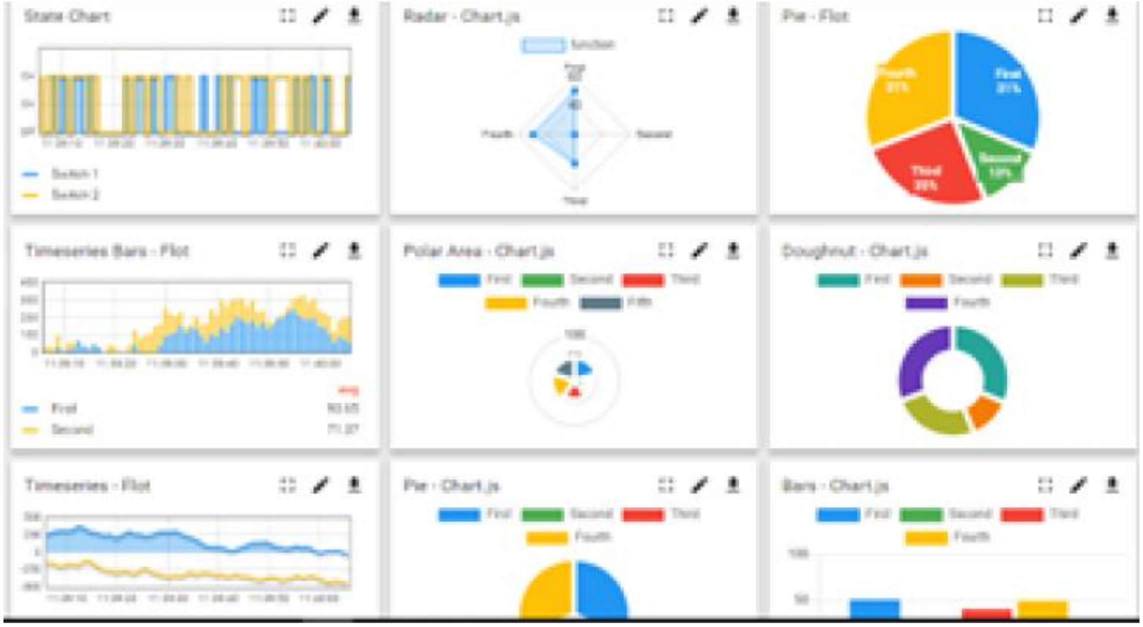
UCT Insight is an IOT platform designed for quick deployment of IOT applications on the same time providing valuable “insight” for your process/business. It has been built in Java for backend and ReactJS for Front end. It has support for MySQL and various NoSql Databases.

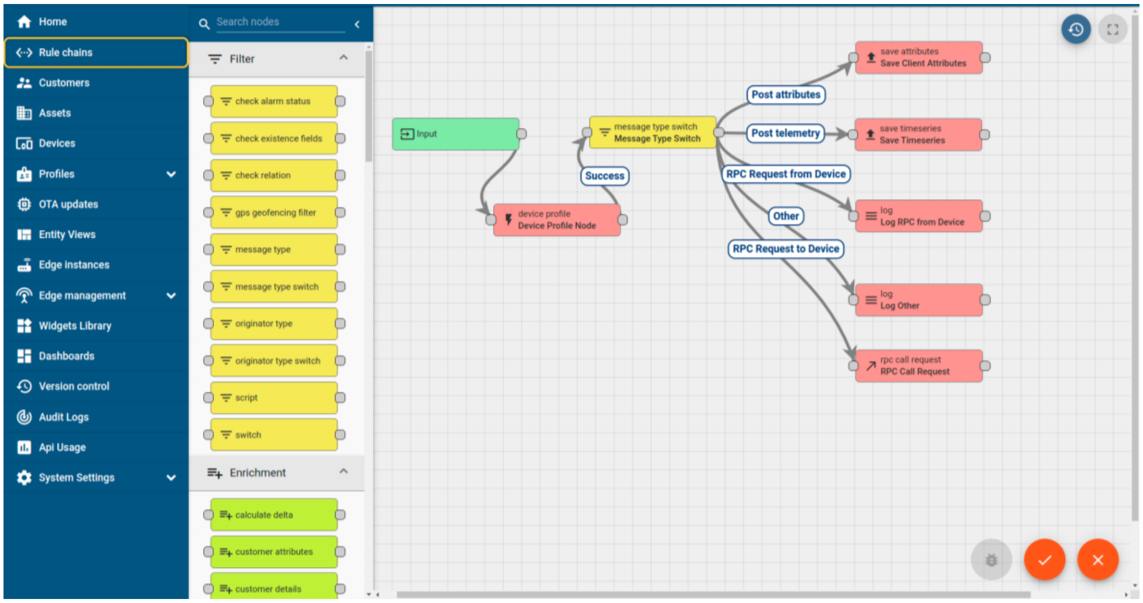
- It enables device connectivity via industry standard IoT protocols - MQTT, CoAP, HTTP, Modbus TCP, OPC UA

- 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


State Chart
Switch 1
Switch 2
Radar - Chart.js
function
First
Second
Third
Fourth
Pie - Flot
Fourth 31%
First 31%
Second 13%
Third 25%
Timeseries Bars - Flot
First
Second
Polar Area - Chart.js
First
Second
Third
Fourth
Fifth
Doughnut - Chart.js
First
Second
Third
Fourth
Timeseries - Flot
Pie - Chart.js
First
Second
Third
Fourth
Bars - Chart.js
First
Second
Third
Fourth
100
50


Home
Rule chains
Customers
Assets
Devices
Profiles
OTA updates
Entity Views
Edge instances
Edge management
Widgets Library
Dashboards
Version control
Audit Logs
Api Usage
System Settings
Search nodes
Filter
check alarm status
check existence fields
check relation
gps geofencing filter
message type
message type switch
originator type
originator type switch
script
switch
Enrichment
calculate delta
customer attributes
customer details
Input
device profile
Device Profile Node
Success
message type switch
Message Type Switch
Post attributes
Post telemetry
RPC Request from Device
Other
RPC Request to Device
save attributes
Save Client Attributes
save timeseries
Save Timeseries
log
Log RPC from Device
log
Log Other
rpc call request
RPC Call Request

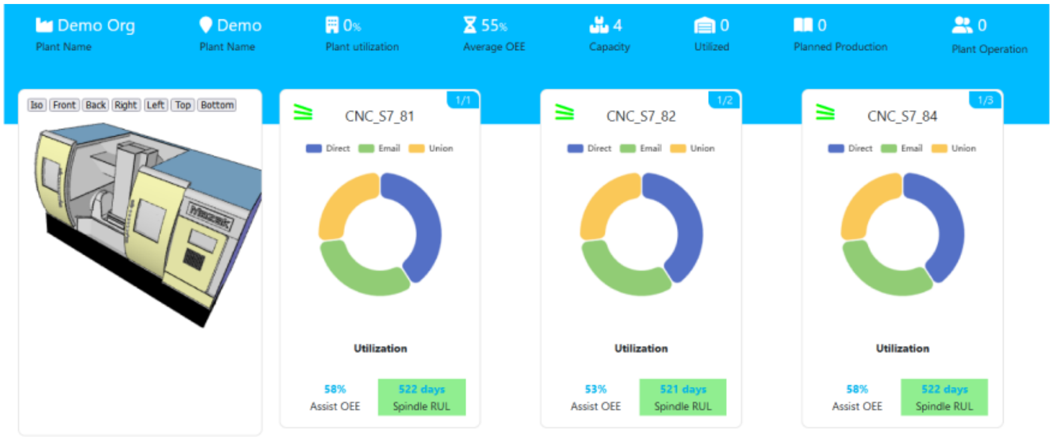
ii. Smart Factory Platform (FACTORY WATCH)

Factory watch is a platform for smart factory needs.

It provides Users/ Factory

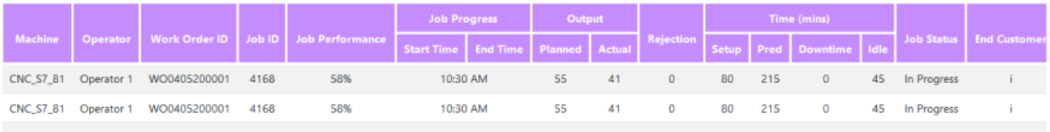
- with a scalable solution for their Production and asset monitoring
- OEE and predictive maintenance solution scaling up to digital twin for your assets.
- to unleased the true potential of the data that their machines are generating and helps to identify the KPIs and also improve them.
- A modular 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.

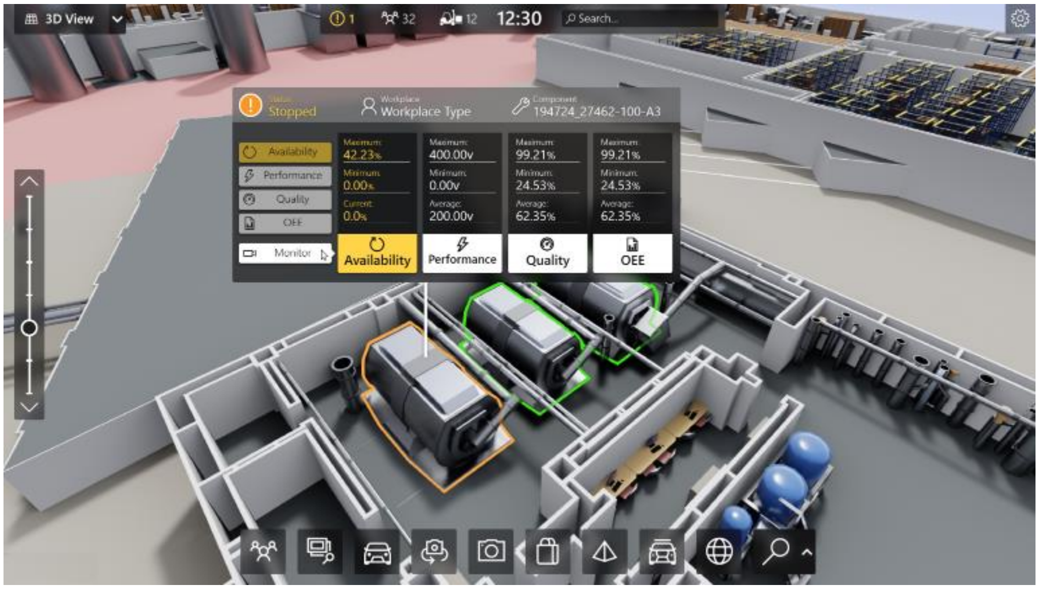


Demo Org — Plant Name
Demo — Plant Name
0% — Plant utilization
55% — Average OEE
4 — Capacity
0 — Utilized
0 — Planned Production
0 — Plant Operation

CNC_S7_81 (1/1): 58% Assist OEE; 522 days Spindle RUL
CNC_S7_82 (1/2): 53% Assist OEE; 521 days Spindle RUL
CNC_S7_84 (1/3): 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

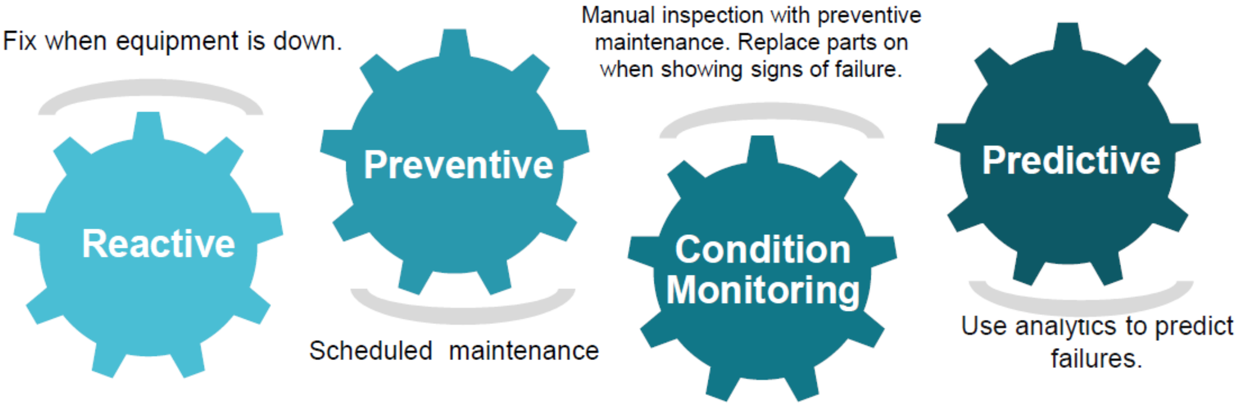
Availability — Maximum: 42.23% Minimum: 0.00% Current: 0.0%
Performance — Maximum: 400.00v Minimum: 0.00v Average: 200.00v
Quality — Maximum: 99.21% Minimum: 24.53% Average: 62.35%
OEE — Maximum: 99.21% Minimum: 24.53% Average: 62.35%

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

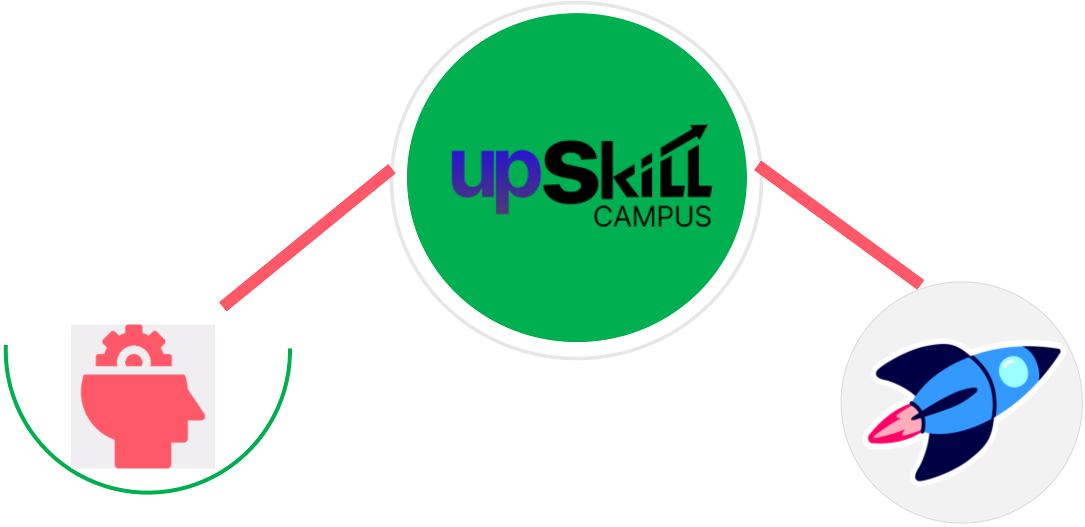
UCT is providing Industrial Machine health monitoring and Predictive maintenance solution leveraging Embedded system, Industrial IoT and Machine Learning Technologies by finding Remaining useful life time of various Machines used in production process.


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.

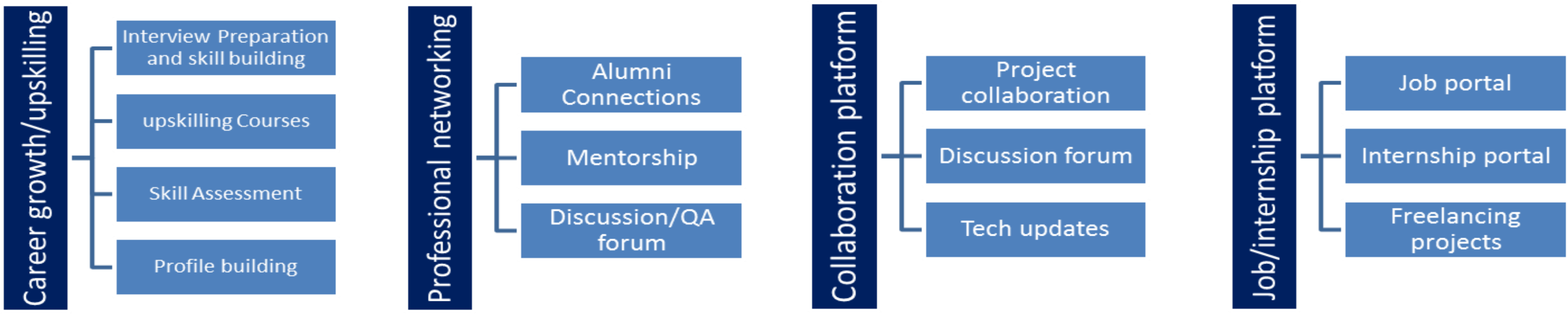
USC is a career development platform that delivers **personalized executive coaching** in a more affordable, scalable and measurable way.



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/



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]

[2]

[3]

2.6 Glossary

Terms	Acronym

3 Problem Statement

In the assigned problem statement

In today's digital age, individuals and organizations face a significant challenge in managing the numerous passwords required for various online accounts and services. With the increasing number of online platforms, the need for strong, unique passwords to protect sensitive information has never been more crucial. However, remembering multiple complex passwords can be difficult, leading to security risks such as using weak passwords, reusing passwords across multiple accounts, or storing them insecurely.

Traditional methods of password management, such as writing passwords down or using easily guessable patterns, are insecure and unreliable. Additionally, relying on browsers to store passwords poses security risks if the device is compromised.

4 Existing and Proposed solution

Provide summary of existing solutions provided by others, what are their limitations?

LastPass:

- LastPass is one of the most popular password managers, offering features like password storage, password generation, and cross-platform accessibility.
- Limitations:

Recent security concerns: LastPass has faced security breaches and concerns regarding its handling of user data, which have raised questions about its overall security.

Password:

- 1Password is known for its strong security features and user-friendly interface, providing password storage, generation, and cross-platform support.
- Limitations:

Limited free version: 1Password offers a limited free version, but its full suite of features requires a subscription, which may not be affordable for all users.

Dashlane:

- Dashlane offers a comprehensive set of features, including password storage, generation, and two-factor authentication support, with a focus on simplicity and security.

- Limitations:
- High pricing: Dashlane's premium subscription can be relatively expensive compared to other password managers, potentially limiting its accessibility to budget-conscious users.

Bitwarden:

- Bitwarden is an open-source password manager known for its security and transparency, offering features like password storage, generation, and cross-platform support.
- Limitations:
- Limited advanced features: While Bitwarden provides essential password management features, it may lack some advanced functionalities compared to other solutions, such as comprehensive security auditing or emergency access features.

What is your proposed solution?

My proposed solution for a password manager would prioritize a balance between security, usability, and accessibility. Here are the key features of the proposed solution:

1. **End-to-End Encryption**: All stored passwords and sensitive data are encrypted locally on the user's device using strong encryption algorithms. This ensures that only the user has access to their data, and even the service provider cannot decrypt it.
2. **Cross-Platform Support**: The password manager should be available on multiple platforms including desktops, smartphones, and web browsers. This ensures seamless access to passwords from any device, enhancing user convenience.
3. **Password Generation**: The solution should offer a built-in password generator capable of creating strong, unique passwords for each account. Users can customize password length, character types, and other parameters according to their preferences.
4. **Two-Factor Authentication (2FA) Integration**: Integration with various 2FA methods adds an extra layer of security to the password manager itself, preventing unauthorized access even if the master password is compromised.

5. **Secure Sharing**: The ability to securely share passwords with trusted individuals or team members without revealing the actual password. This feature ensures collaboration without compromising security.
6. **Auditing and Monitoring**: Regularly audit password strength and identify potential security vulnerabilities. Alerts can be provided to users for weak or reused passwords, prompting them to update them for improved security.
7. **Emergency Access**: Implement a mechanism for granting emergency access to trusted individuals in case the user is unable to access their account due to unforeseen circumstances. This ensures continuity of access while maintaining security.
8. **Backup and Sync**: Automatic backup and synchronization of encrypted password data across devices to prevent data loss and ensure accessibility. Users have the option to manually trigger backups or choose backup locations.
9. **User-Friendly Interface**: A clean and intuitive user interface that makes it easy for users to add, manage, and retrieve passwords. Features such as browser extensions, autofill, and quick search enhance user experience and efficiency.
10. **Privacy-Focused**: Commitment to user privacy by minimizing data collection, implementing transparent privacy policies, and offering options for users to control their data.
11. **Affordability and Accessibility**: Offer a range of pricing plans, including a free tier with essential features and premium tiers with advanced functionalities. The solution should be accessible to users with different budget constraints.

What value addition are you planning?

Improving password manager capabilities can include several value additions:

1. **Enhanced Security Features**: Implementing advanced encryption methods, biometric authentication, and multi-factor authentication (MFA) options can significantly enhance security.
2. **Intelligent Password Generation**: Integrating AI to suggest strong, unique passwords tailored to individual users' preferences and security needs can simplify password management.

3. **Cross-Platform Integration**: Expanding compatibility across various devices and platforms ensures seamless access to passwords and data anywhere, anytime.
4. **Secure Sharing**: Introducing secure sharing options for passwords and sensitive information with trusted individuals or teams, while maintaining strict access controls.
5. **Password Health Monitoring**: Providing insights and alerts on weak, reused, or compromised passwords to encourage better password hygiene.

4.1 Code submission (Github link)

https://github.com/Ludhiya-123/Password-Manager.upskills-Campus.git

4.2 Report submission (Github link) **:** first make placeholder, copy the link.

5 Proposed Design/ Model

Given more details about design flow of your solution. This is applicable for all domains. DS/ML Students can cover it after they have their algorithm implementation. There is always a start, intermediate stages and then final outcome.

5.1 High Level Diagram (if applicable)

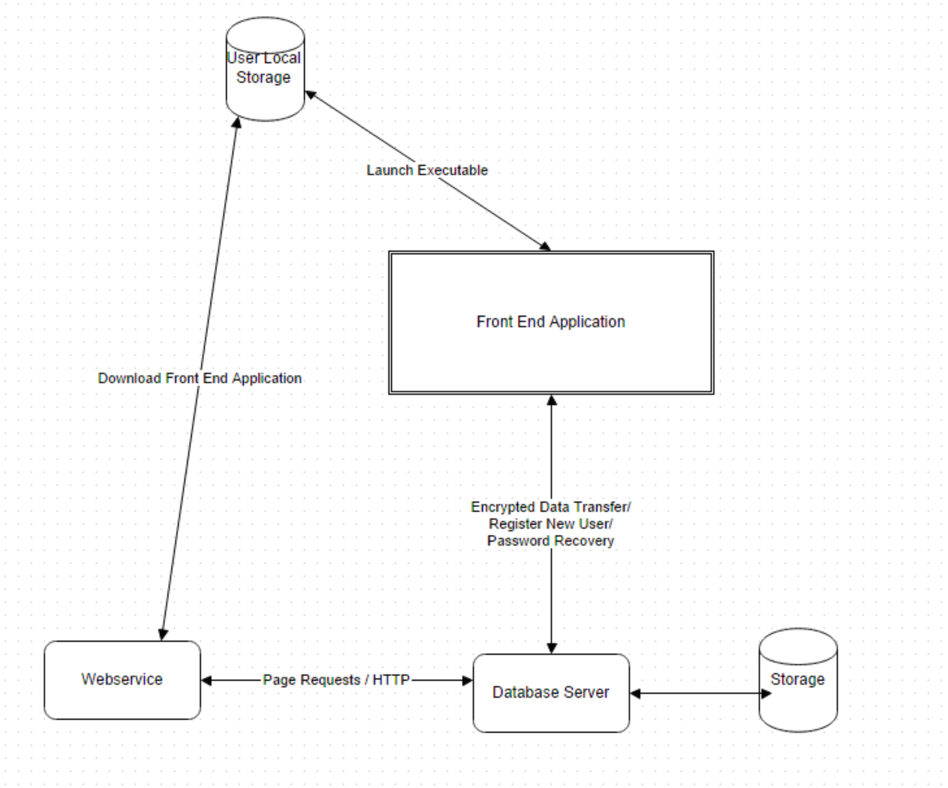
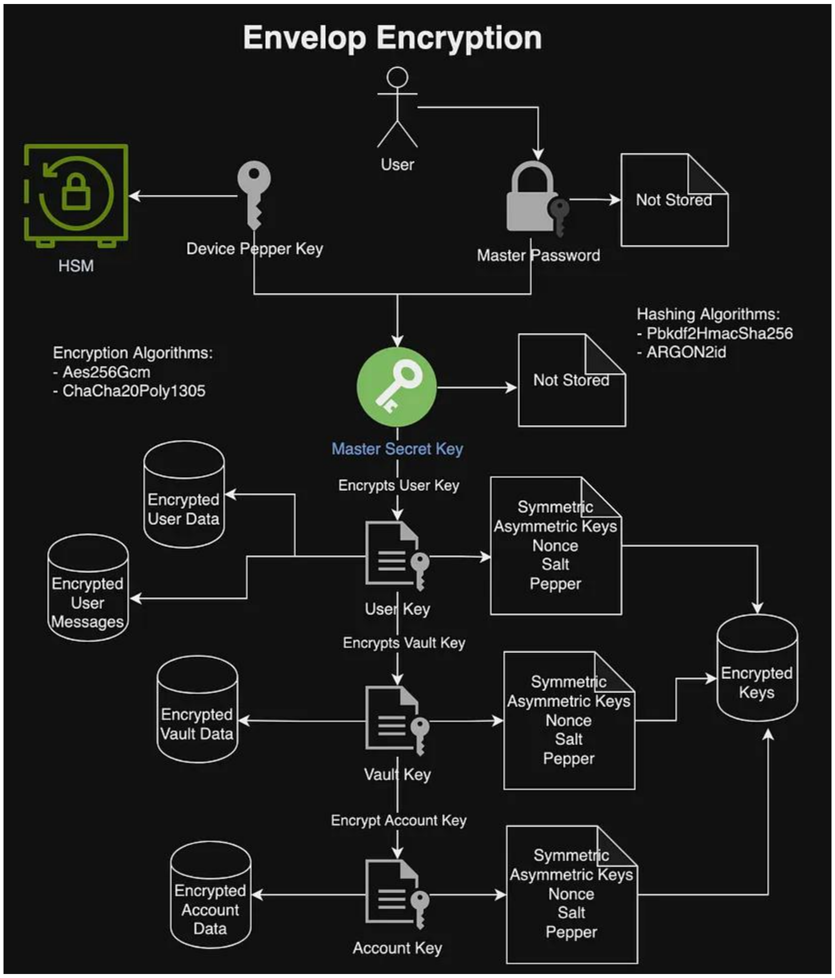


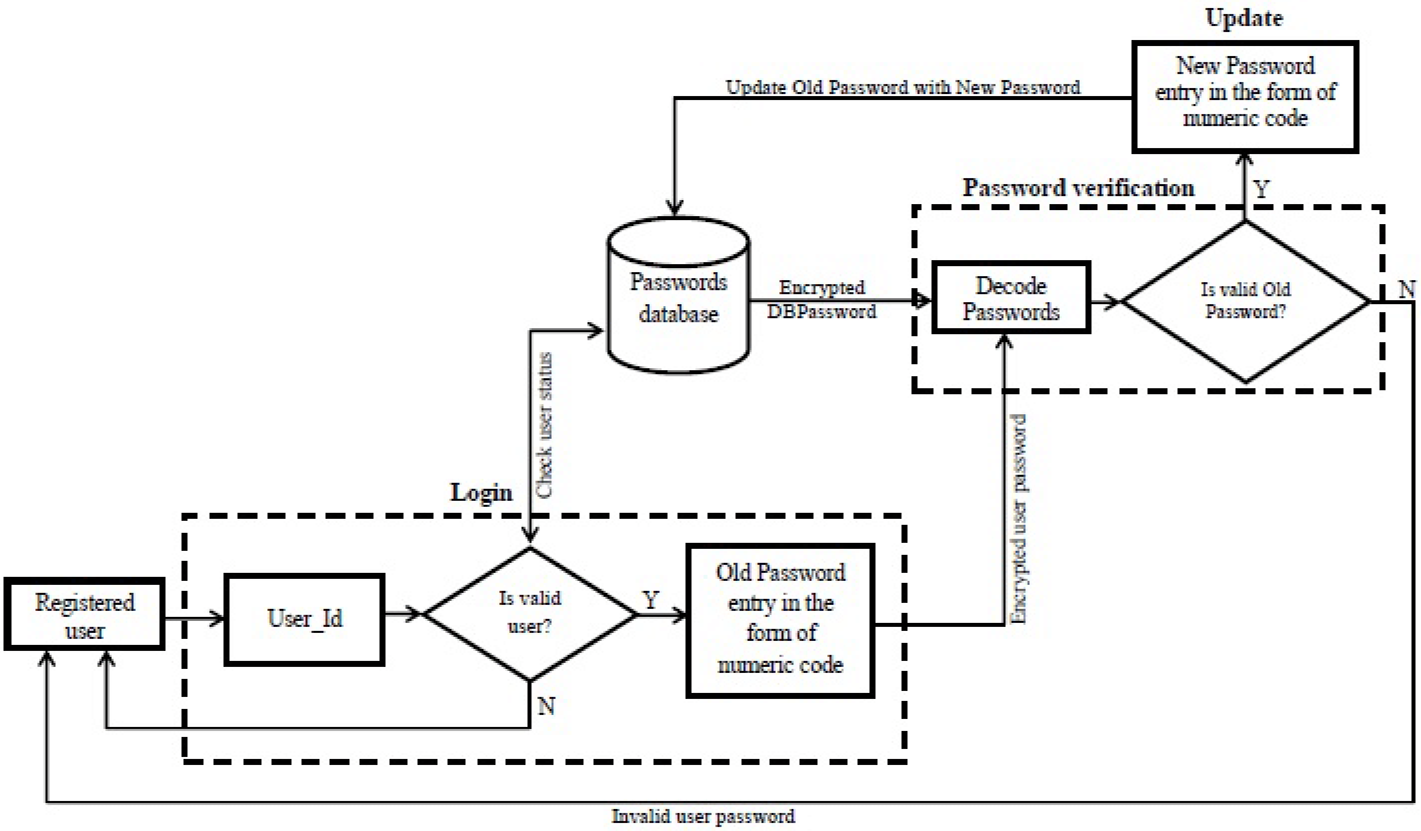
Figure 1: HIGH LEVEL DIAGRAM OF THE SYSTEM

5.2 Low Level Diagram (if applicable)



5.3 Interfaces (if applicable)

Update with Block Diagrams, Data flow, protocols, FLOW Charts, State Machines, Memory Buffer Management.



6 Performance Test

This is very important part and defines why this work is meant of Real industries, instead of being just academic project.

Here we need to first find the constraints.

How those constraints were taken care in your design?

What were test results around those constraints?

Constraints can be e.g. memory, MIPS (speed, operations per second), accuracy, durability, power consumption etc.

In case you could not test them, but still you should mention how identified constraints can impact your design, and what are recommendations to handle them.

6.1 Test Plan/ Test Cases

- Verify if a valid password is allowing users to successfully log in to their accounts.
- Check if an invalid password entry is preventing users from logging into the account.
- Check if an error message displays when the entered password is wrong.
- Validate that the password field is case-sensitive.
- Verify the size, font, and placement of the password input field on the page.
- Check that the entered password is not visible at first and is hidden by some special characters (dots, asterisk, or such).
- Test if the option to make the password visible (usually, *Show Password)* is present or not.
- Test if clicking on the *Show Password* button makes the password visible to the user.

6.2 Test Procedure

- Setting up an account
- Creating a master password
- Watching/reading instructional content
- Encrypting files
- Sharing files
- Adding browser extensions
- Installing mobile apps
- Adding passwords (either through a browser extension or manually)
- Importing and exporting passwords
- Generating passwords
- Checking password strength
- Auto filling passwords
- Configuring 2FA and/or biometric authentication
- Using additional features

6.3 Performance Outcome

Password vaults or *password managers* are programs that keep your passwords in a secure location. When you use this software, the passwords are encrypted, and you use a single master password to access them. Depending on the tool being used, these passwords may be stored on a secure website, or on your local computer. In using it, you only need to remember one password to view the database of other passwords for various sites and apps. Some of the password managers available include

- LastPass (https://lastpass.com)

RoboForm (www.roboform.com)
Each of the above-mentioned tools are free, although premium versions can be purchased. Both have versions available that work with mobile devices and Windows computers, while RoboForm also has a version that works with Macs. By installing an extension to your browser, you navigate to a site, enter your username and password, and have the option to save it to the password manager. After this, you can navigate to the bookmarked sites and automatically login.

7 My learnings

I am thrilled to share that I have successfully completed my internship on Python. This opportunity has allowed me to expand my skills and knowledge in the field and gain valuable experience. I am grateful for the chance to work with such a talented team and for the support and guidance provided through my internship.

I have learned many things and done weekly reports. And learned Advanced topics using Python.

8 Future work scope

This Internship give me a taste of what working in a particular role or field .

It helps me how to complete projects and how to crack the jobs with these technical skills.