Industrial Internship Report on

”Password Manager”

Prepared by

[Krutika Kandalkar]

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 Python Project provided by UCT. We had to finish the project including the report in 6 weeks’ time.

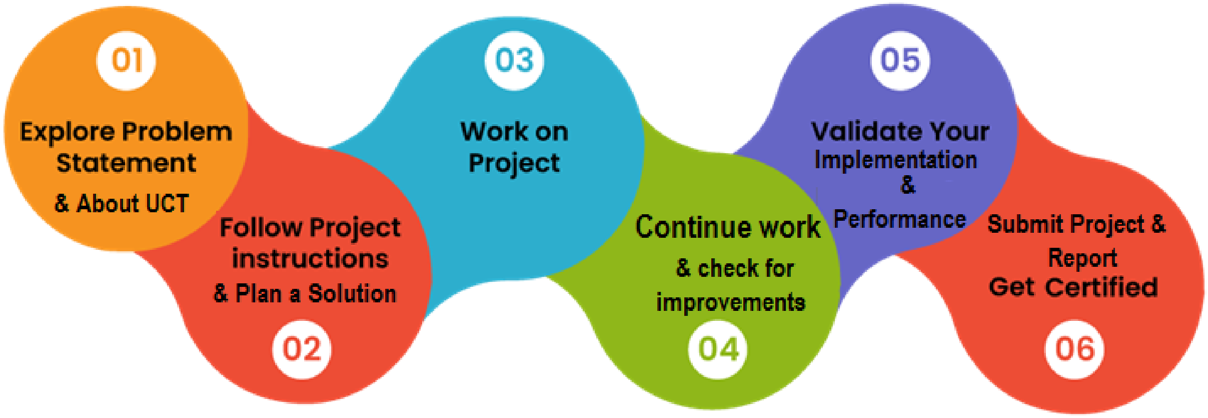
My project was The password manager is a Python project that securely stores and manages user passwords. It allows users to store their passwords for various accounts, generate strong passwords, and retrieve passwords when needed.

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

There is a introductory part like the basics of Python for Data Science, python applications like Data Analysis, Web Development, Scripting and Automation, characteristics of Python, Python Library. There is a conditional statement in Python like If , If Else and If Elif Else. And solve the test where some coding questions are given and theory questions are also there. I learned about the Numpy, Introduction to Numpy, different Numpy operations, Introduction to Pandas and Operations.



01 Explore Problem Statement & About UCT

02 Follow Project instructions & Plan a Solution

03 Work on Project

04 Continue work & check for improvements

05 Validate Your Implementation & Performance

06 Submit Project & Report Get Certified

The overall experience is great. I have developed a positive attitude, and a strong sense of responsibility, being innovative, resourceful, open, and responsive to changes. It has created in me an interest in lifelong learning.

Thanks to all the UpSkill Campus Team who have helped me directly or indirectly.

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

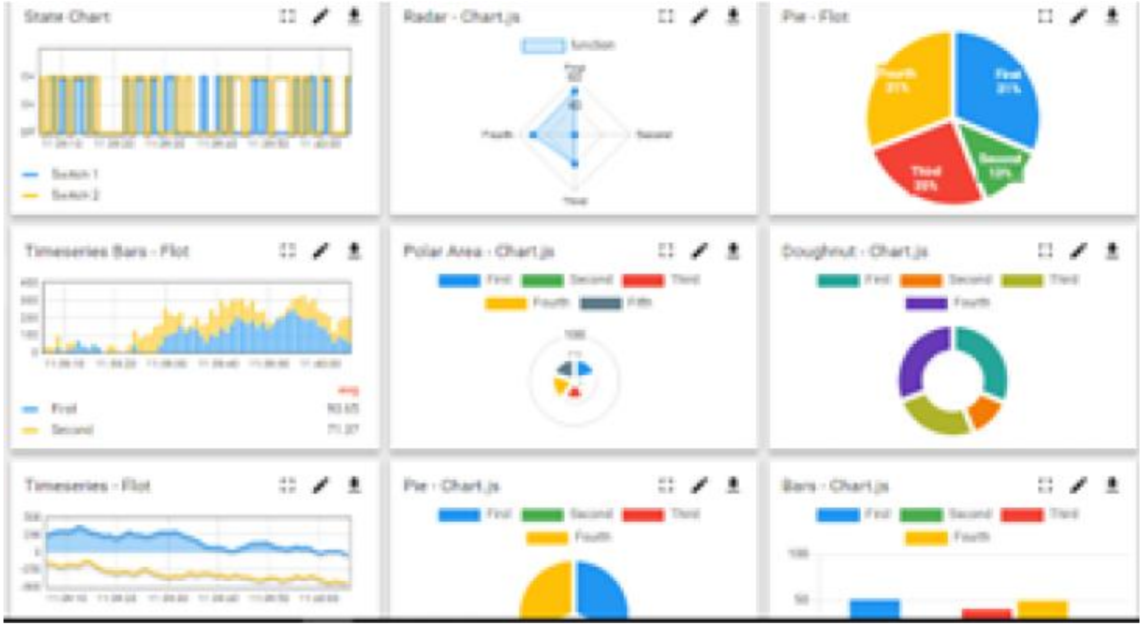
UCT Insight is an IOT platform designed for quick deployment of IOT applications on the same time providing valuable “insight” for your process/business. It has been built in Java for backend and ReactJS for Front end. It has support for MySQL and various NoSql Databases.

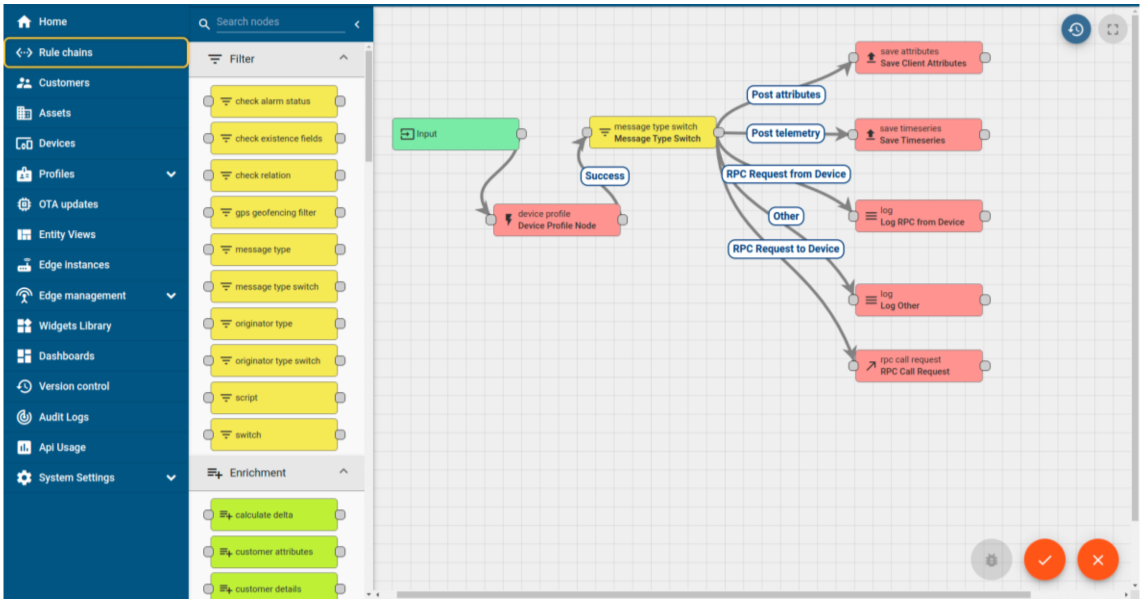
- It enables device connectivity via industry standard IoT protocols - MQTT, CoAP, HTTP, Modbus TCP, OPC UA

- 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%
Third 26%
Second 13%
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


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
message type switch
Message Type Switch
Success
device profile
Device Profile Node
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

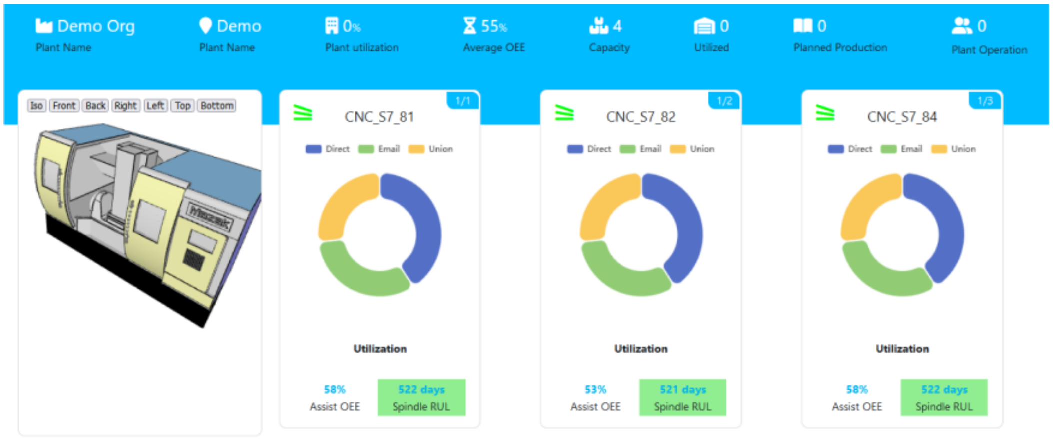
ii. Smart Factory Platform (FACTORY WATCH)

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.

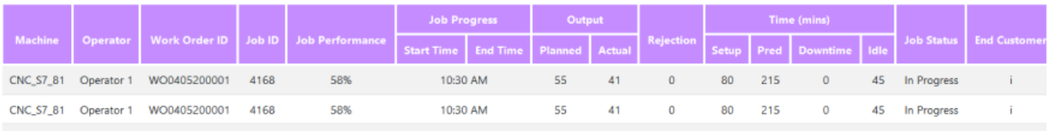


Demo Org Plant Name | Demo Plant Name | 0% Plant utilization | 55% Average OEE | 4 Capacity | 0 Utilized | 0 Planned Production | 0 Plant Operation

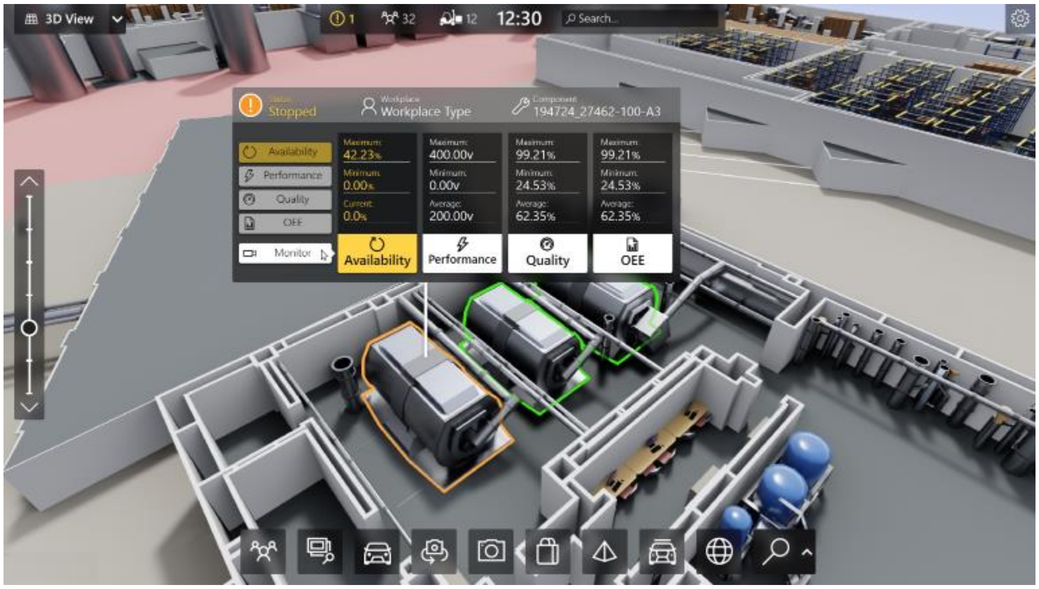
CNC_S7_81: 58% Assist OEE, 522 days Spindle RUL

CNC_S7_82: 53% Assist OEE, 521 days Spindle RUL

CNC_S7_84: 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

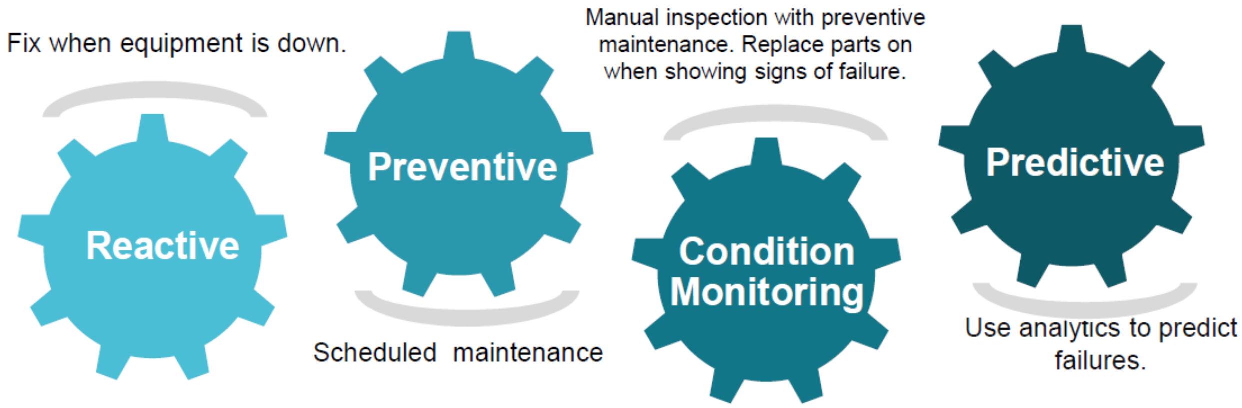
Availability	Performance	Quality	OEE
Maximum: 42.23%	Maximum: 400.00v	Maximum: 99.21%	Maximum: 99.21%
Minimum: 0.00%	Minimum: 0.00v	Minimum: 24.53%	Minimum: 24.53%
Current: 0.0%	Average: 200.00v	Average: 62.35%	Average: 62.35%

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

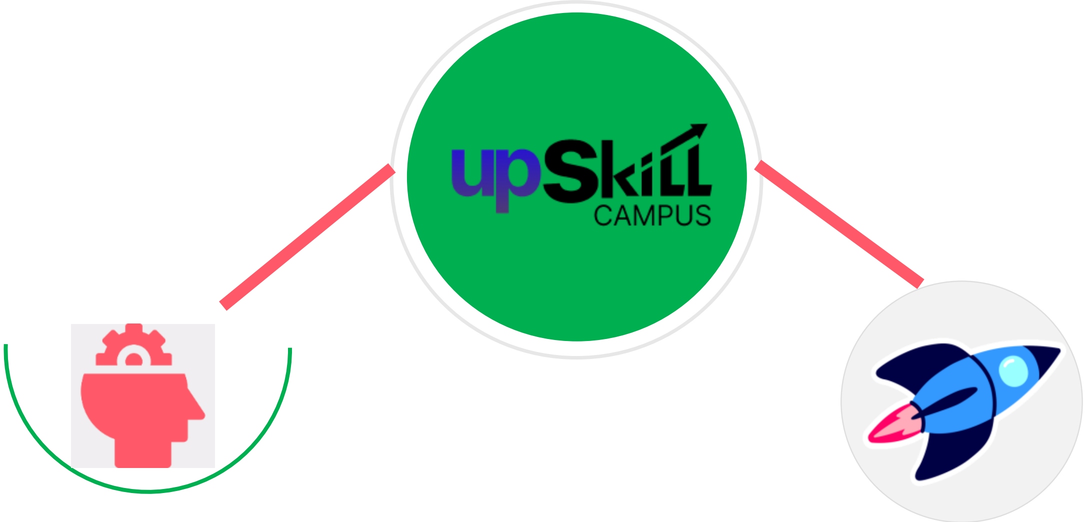
UCT is providing Industrial Machine health monitoring and Predictive maintenance solution leveraging Embedded system, Industrial IoT and Machine Learning Technologies by finding Remaining useful life time of various Machines used in production process.


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.

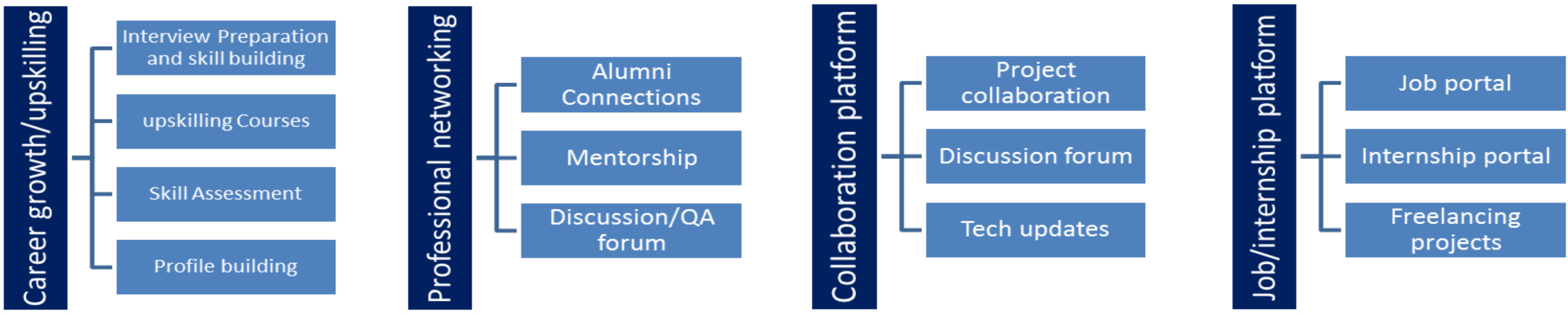
USC is a career development platform that delivers **personalized executive coaching** in a more affordable, scalable and measurable way.



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/



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] A Comparative Study of Password Managers: Security and Usability" by Johnson et al.

(2017)

[2] User Perception and Adoption of Password Managers: A User Study" by Smith and Brown

(2018)

[3] Enhancing Password Manager Security with Two-Factor Authentication" by Chen et al.

(2019)

3 Problem Statement

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.

Individuals and organizations alike have to manage an increasing number of passwords for various online accounts and services. The use of weak passwords or reusing the same password across multiple accounts can compromise security and lead to data breaches. Furthermore, remembering multiple complex passwords can be a daunting task, leading to the risk of losing access to important accounts or being locked out. Password management tools aim to solve these issues by providing a secure and convenient way to store and manage passwords.

However, the increasing number of password management tools available in the market can make it difficult for individuals and organizations to choose the right tool that fits their needs. Furthermore, concerns around the security of the password management tool itself, the potential for the tool to be a single point of failure, and the risk of losing access to all accounts if the master password is forgotten or compromised also exist.

Therefore, the problem statement is to identify and evaluate the effectiveness and security of password management tools and develop best practices for their implementation, use, and maintenance. Additionally, it is essential to understand the user requirements and preferences for password management tools and develop solutions that balance convenience and security

4 Existing and Proposed solution

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.

4.1Code submission (Github link)

https://github.com/Krutika2012/upskillCampus

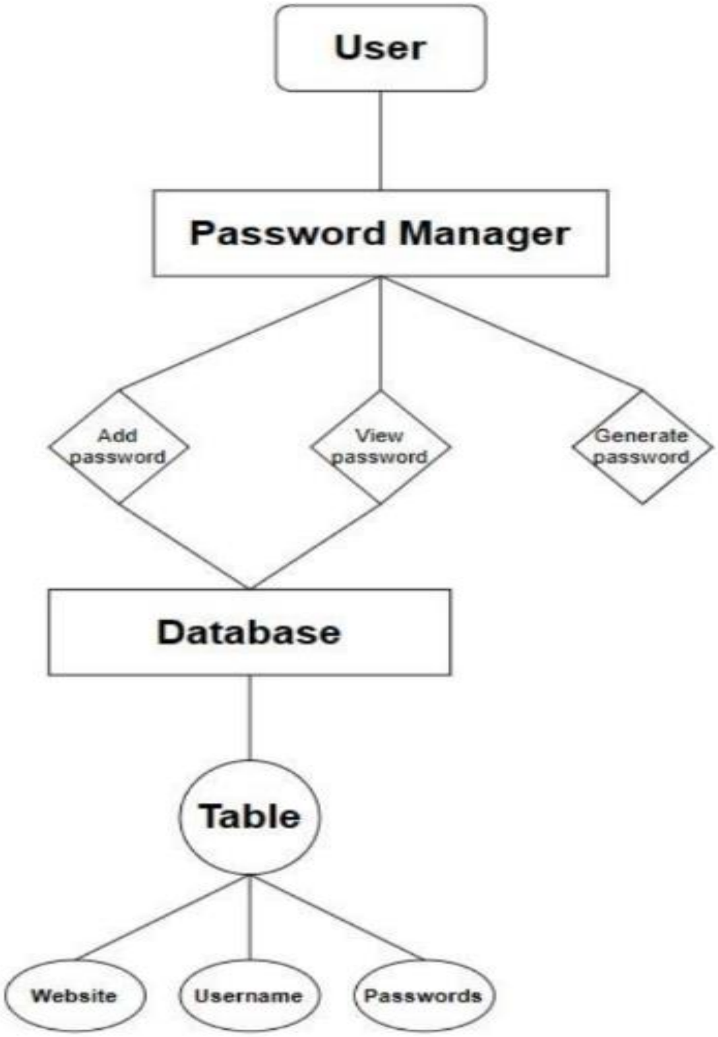
4.2Report submission (Github link) :

https://github.com/Krutika2012/upskillCampus

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 Interfaces (if applicable)



6 Performance Test

when we start up our password management web application, this home page is loaded up to greet the users. The code of the homepage template is stored in a file called index.html which is loaded up to greet the user whenever the web application is started. Users can click on the Get Started button to be navigated to the next webpage where passwords can be added to the MySQL database using an add_password() function.

Alternatively, users can navigate to the other webpages using the hyperlinks provided on the top right corner of the webpage where links to the homepage, add password webpage and view passwords webpage are provided.

The user will be required to enter a website name, user name and a password. If any of the above-mentioned fields are left empty, an error will be shown prompting the user to fill all the necessary fields before continuing. Once all the fields are filled the details will be added to the MySQL database.

The password added to the MySQL database will be encrypted using a python cryptography library so that even if the database is compromised, the passwords will still stay secure as the decryption key will not be saved in the database and the passwords can not be viewed as plaintext without the encryption key.

7 My learnings

Creating a password management solution is a crucial component of contemporary cybersecurity. This project is intended for people who often use the internet, create several online accounts, and find it difficult to remember all of their account's login information, due to the rising number of the accounts and the complexity of passwords. And due to the increased danger of using weak passwords or the same password for several accounts, users are more likely to become the target of hacking efforts.

By giving users a safe and convenient way to save and manage their passwords, the adoption of a password management application can help reduce these risks. The program may assist users in creating unique, secure passwords and remembering them without the need to memorize or write them down thanks to features like password creation, storage, and auto-filling. A password management tool has a bright future ahead of it because to prospective features like biometric verification, password sharing, and cloud-based storage. These improvements might improve the tool's ease, security, and usability, increasing its value to users.

Overall, using a password management solution is a crucial step towards enhancing online security and lowering the dangers connected to using default or weak passwords. Such a solution can give consumers a safer and more effective method to manage their passwords by including best practices and new technology

8 Future work scope

Since the necessity for strong and secure passwords is growing in importance in the current digital age, the future potential for a password management tool project is highly promising. Here are some potential directions for this project's future growth and development:

- Integration with many devices: Given how many devices people use on a daily basis, a password management application must be usable on a variety of platforms, including desktop, mobile, and tablet.

- Biometric authentication: To provide an additional layer of protection to password management software, biometric authentication methods such as voice recognition, fingerprint scanning, and face recognition may be included.

Password sharing: Ability to share password between trustworthy individuals or members of a team is a helpful feature that might be added to password management software to make it simpler for teams to work together securely.

- Analysis of password strength: It is crucial for password management software to be able to assess the strength of users' passwords and provide recommendations for strengthening them as cybersecurity threats change.

- Cloud-based storage: By implementing cloud-based storage, users will be able to safely save their passwords and get access to them whenever and wherever they choose.

- Two-factor authentication: As an additional security measure, two-factor authentication is gaining popularity. It could be beneficial to incorporate this functionality into password management software.

Overall, the future scope of password management tools is vast, and there is room for innovation and improvement in many areas.