Industrial Internship Report on

”Password Manager”

Prepared by

Soorya U

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 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

Brief about my project , Program plan and summary of 6 weeks' work :

First we implemented hashing function , where hashing is an algorithm converts data into a fixed-length hash value, hash code, or hash. In essence, the output hash value is a summary of the original value. These hash values are important because they cannot be used to retrieve the original input data.

On week 02 we applied code which generates an unique key, Encrypts the given password and decrypts the encrypted password .Encryption is the method by which information is converted into secret code that hides the information's true meaning.

Lately by week 03 we stepped into Structured query language (SQL) ,It is a programming language for storing and processing information in a relational database. we used SQL statements to store, update, remove, search, and retrieve information from the database and also to maintain and optimize database performance.

At the last week we worked on Tkinter which is popularised as one of the GUI application. Tkinter is the inbuilt python module that is used as one of the most commonly used modules for creating GUI applications in Python as it is simple and easy to work with.

About need of relevant Internship in career development :

Just having a good degree is no longer enough to secure that all-important graduate job offer in today's world. Pertinent work experience is now just as valuable as your degree and exam results when it comes to building a successful career. As a result, internships have become an essential way to help candidates make themselves stand out.

Opportunity given by UCT/USC:

They offer organizations across the world, a wide gamut of services and solutions in the Wireless Communication and IOT domain and free Internship projects for student's to improve their skills.

Experience and Greetings: Overall, my internship at Upskill campus was a valuable learning experience. Firstly I thank UCT/USC IoT Platform for this best opportunity .Thank you Saanvi MJ, Modhak V Raj and Hamsa CS for being my teammates , helping out each other throughout this project

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)

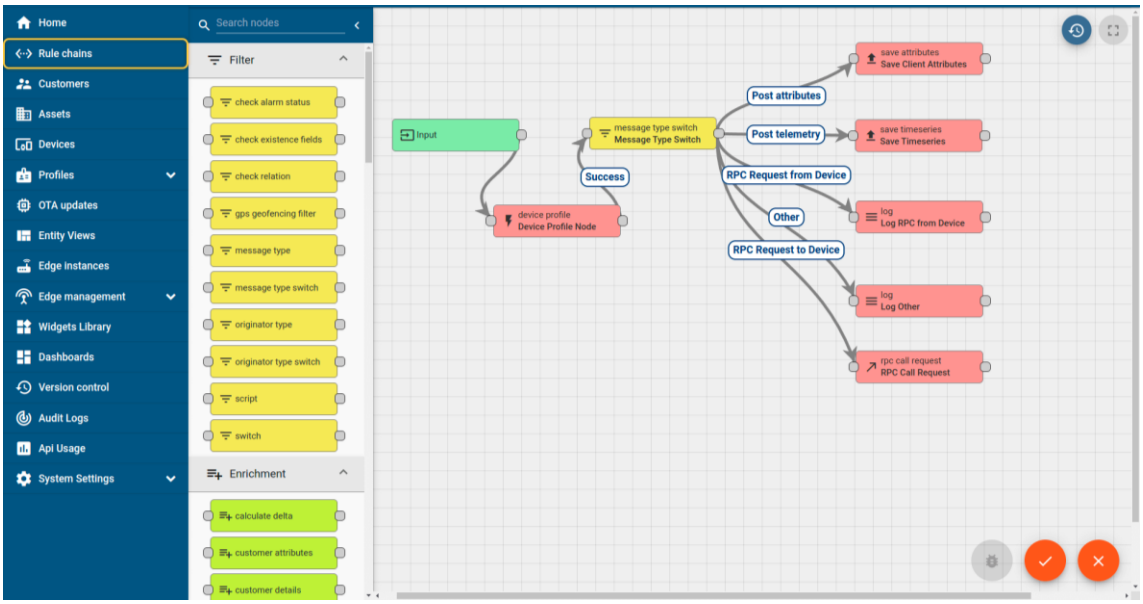
UCT Insight is an IOT platform designed for quick deployment of IOT applications on the same time providing valuable "insight" for your process/business. It has been built in Java for backend and ReactJS for Front end. It has support for MySQL and various NoSql Databases.

- 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.

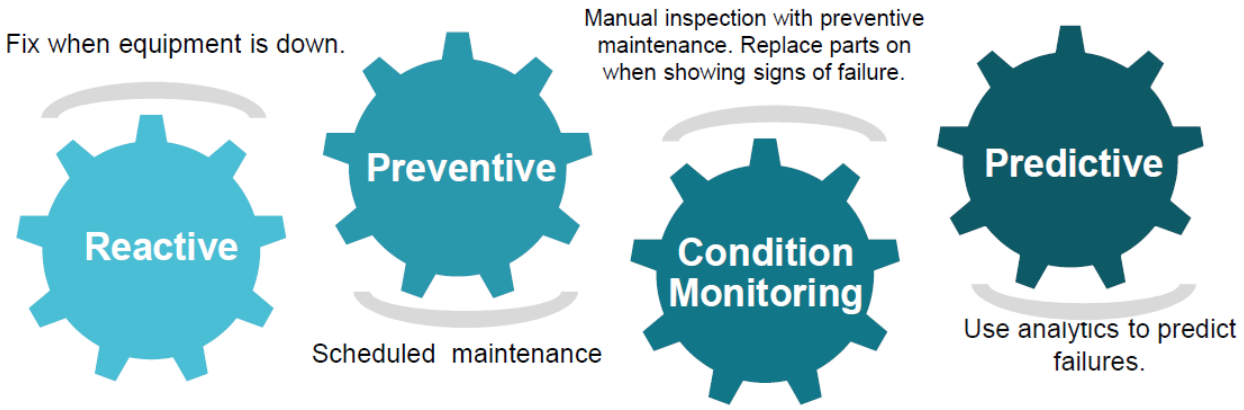
Machine	Operator	Work Order ID	Job ID	Job Performance	Job Progress		Output		Rejection	Time (mins)				Job Status	End Customer
					Start Time	End Time	Planned	Actual		Setup	Pred	Downtime	Idle		
CNC_S7_81	Operator 1	WO0405200001	4168	58%	10:30 AM		55	41	0	80	215	0	45	In Progress	i
CNC_S7_81	Operator 1	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 technology and providing solution in Agritech, Smart cities, Industrial Monitoring, Smart Street Light, Smart Water/ Gas/ Electricity metering solutions etc.

iv. Predictive Maintenance

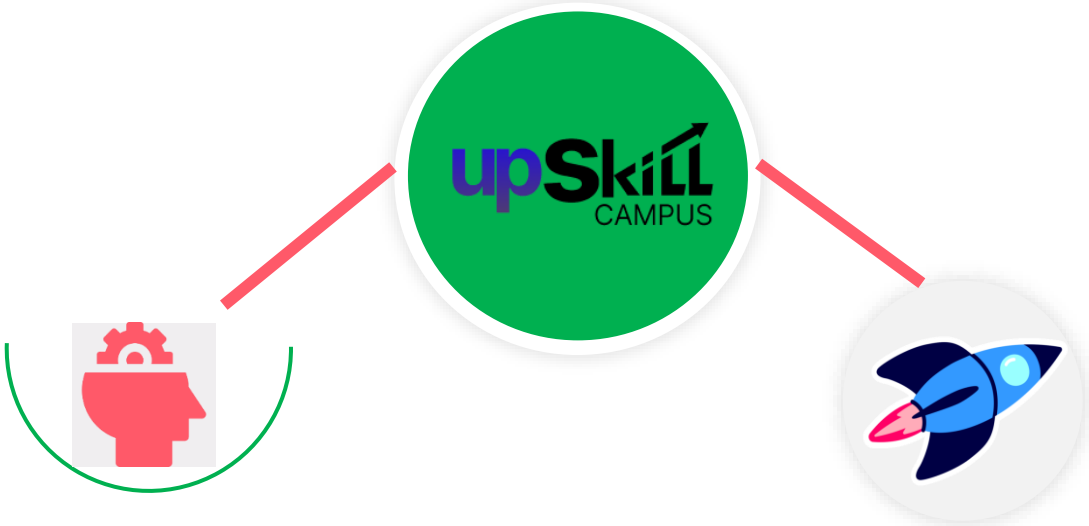
UCT is providing Industrial Machine health monitoring and Predictive maintenance solution leveraging Embedded system, Industrial IoT and Machine Learning Technologies by finding Remaining useful life time of various Machines used in production process.



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.

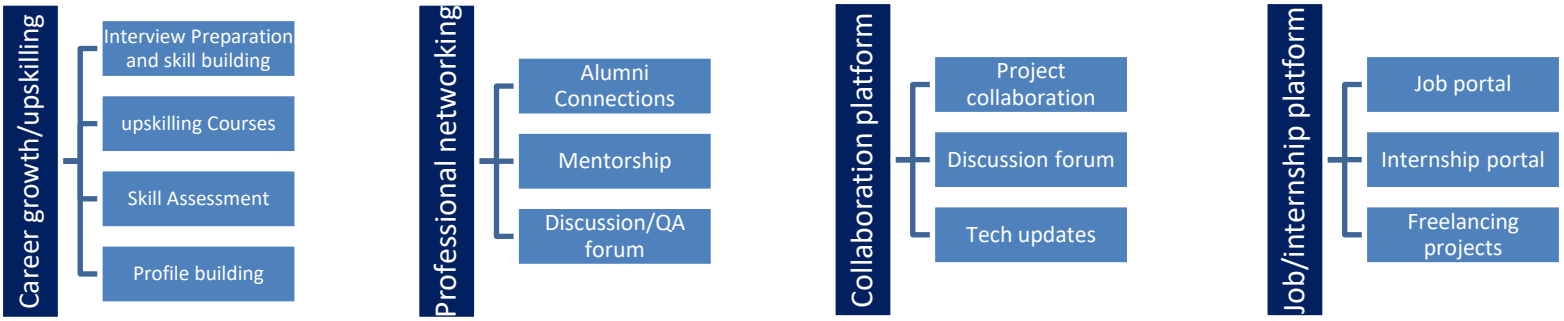
USC is a career development platform that delivers **personalized executive coaching** in a more affordable, scalable and measurable way.



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/



2.3 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.

2.4 Reference

[1] Google

[2] YouTube

[3] Wikipedia

2.5 Glossary

Terms	Acronym
SQL	Structured Query Language
Db	Database

3 Problem Statement

Passwords are annoying to keep track of manually and are the most vulnerable link in the security chain. Even the best Android phones can only partially protect us from weak passwords. Proper cybersecurity protocols must be in place since we rely on the internet more now than in the past. In comes password manager services with features such as safely storing our passwords, one-tap logins, and unique password generation. When you use everything they offer, you'll never want to go back to trying to remember or writing down your passwords.

There's only one password to remember

Since we have to create a new password for every account we make online, keeping track of each one can become a chore. Although a red flag for security reasons, some people reuse or share passwords for multiple accounts without thinking twice.

The chances are low that the average user will be interested in using a unique password for each account while remembering them all. A benefit to a password manager is that you only need to keep track of a single primary password. Nothing more, nothing less.

There are still people in 2022 who continue using phrases such as 123456, password, and qwerty to protect their accounts. This is scary and concerning in our modern smartphone era, where everything we do is online. Our smartphones house private and personal information unique to us as individuals, including messages, contacts, photos, and videos. And many of us access our bank accounts and credit cards using their respective apps. Not securing your account login information is risky, more so now than ever before, as we have shifted to a mobile-first world.

You can increase your password strength by combining uppercase and lowercase letters with a random assortment of symbols. A password manager can do this for you to generate unique passwords for each of your accounts. You won't even know your passwords, which is what you want since you'll be saving them to your password manager. You'll be able to lock them behind your biometrics and autofill them when needed, giving you the best of both worlds. This helps bridge the security gap until we can do away with passwords for good in the future.

Your passwords are safely stored and encrypted

Keeping your saved card passwords or credit numbers in a plain text file on your computer isn't the safest way to store them, especially since it's unencrypted. Anyone with access to your computer, either locally

or remotely, can open the document and view your account credentials with zero effort. And it doesn't matter how strong or weak your passwords are. They will be immediately exposed in easy-to-read text.

A password manager stores your passwords using the highest level of encryption, keeping them safe from outside threats. This includes hackers and malware infections looking to swipe your personal details without your knowledge. With phishing attacks, data breaches, and identity theft on the rise, you'll want to guard yourself against all potential online threats and vulnerabilities. Most modern password managers support the latest AES 256-bit encryption, which uses a 256-bit key length to encrypt and decrypt your data safely.

What's a good free password manager?

Some have advised against using free built-in password managers in the past, but that's less of an issue today. Google's Password Manager, for example, is free to use with your Google account and offers various features to improve your experience. You can generate strong passwords by tapping a button, get notified if your passwords have been compromised, and access your passwords across all major platforms. Using an iPhone, you can autofill your iOS app and website logins via Chrome to make your life easier. No more typing them in or using the Apple Safari web browser.

Using a password manager will enhance your login experience

When it comes down to it, there's no such thing as a good password, regardless of how complex you make them. Using a password manager has many benefits, allowing you to ditch the old way of doing things without looking back. They are designed to protect your online digital life, from securely storing your passwords to using the autofill feature for easy account logins.

4 Existing and Proposed solution

Password managers typically offer spaces for employees to separate personal and business credentials to help ensure employees don't leak or leave with sensitive business information and intellectual property. The best password managers also help IT monitor and measure security performance by creating a security score based on metrics like password reuse across business and personal accounts. Password managers free employees from having to remember (or write down) dozens of passwords. They also enable co-workers to securely share passwords, lessening the likelihood of a data breach

HOW COMPANIES MANAGE PASSWORDS 59% Human memory ,42% Sticky notes,36% Browser extensions, 31% Password manager .29% solution Spreadsheet.

Their limitations

THE ADOPTION AVERSION PROBLEM

Despite steadily rising risks and costs associated with password-related security incidents, IT leaders may find it difficult to justify the time and costs needed to implement a password management solution. Here are the four most common roadblocks to the adoption of password managers.

INITIAL VALUE COMPREHENSION :It's challenging to quantify the value of certain security technologies because business leaders cannot accurately predict the likelihood, extent, or cost of a data breach. Often, the deciding factor in deploying a password management solution is a breach to the organization itself or high-profile attacks on industry peers. Ponemon, in fact, found that 65% of businesses updated password management capabilities only after an attack.

RISK OF PROJECT FAILURE: Another concern, one that most IT leaders know all too well, is the risk of project failure. In general, a fast and efficient software implementation elicits little response. But a problematic, disruptive deployment is likely to spark comments across the enterprise, from new employees to seasoned C-suite executives.

SOLUTION ADOPTION: Even the simplest implementations are not immune to resistance. Initially, some employees will find password managers frustrating to use, while others simply may not trust the technology. No matter the misgiving, user adoption is critical to success and is an initiative that warrants careful planning and employee training.

EXECUTIVE BUY-IN AND SUPPORT: Another people-related challenge lies in obtaining buy-in and support from executive leaders and the board of directors. Security is an enterprise-wide risk-management effort; it requires proactive support that starts in the C-suite and cascades down to all divisions and employees.

Solution proposed:

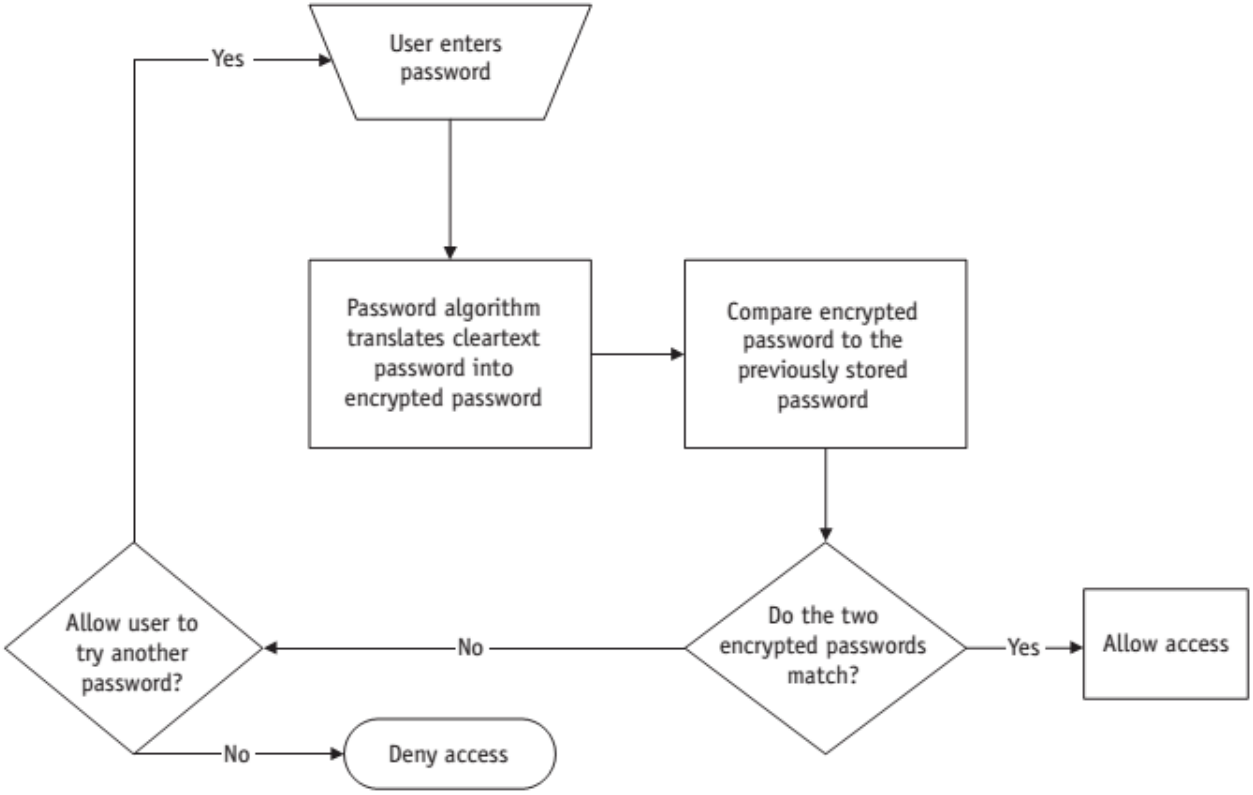
A state-of-the-art password manager should rate the strength of user passwords and help identify and support best practices for creating more robust credentials. In general, strong password policies should:

1. Use a mix of character types, such as at least one number, uppercase letter, and symbol Have a minimum of eight characters; longer passwords are less vulnerable to brute-force attacks Avoid words that can be found in a dictionary, are variations on a user's name, or riffs on personal information such as the name of a child or pet
2. The storage of these passwords—either on premises or in the cloud—is a critical decision. IT leaders should balance the pros and cons of each method to better align password management tools with existing security systems and processes. While there's no universal approach, a password manager that offers a choice between cloud and local storage can provide enhanced flexibility
3. Best-in-class password protection solutions use zeroknowledge architecture that syncs encrypted data in the cloud and decrypts it on the user's local device. Passwords saved in a zero-knowledge architecture allow the business to evaluate the strength of any password without actually knowing any information about the password itself. What's more, a zero-knowledge approach limits access to data encryption keys to the business; the service provider cannot access encryption keys and therefore cannot access stored data.

4.1 Code submission : soorya-u/upskill_campus (github.com)

4.2 Report submission (Github link) : soorya-u (Soorya U) (github.com)

5 Proposed Design/ Model

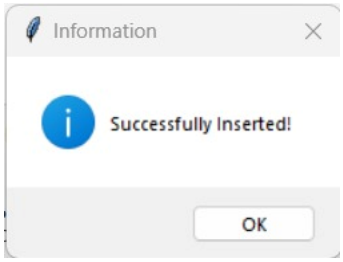


6 Performance Test

6.1 Test Plan/ Test Cases

- Tkinter
- SQL
- Cryptography
- Hashing

6.2 Performance Outcome



7 My learnings

Tkinter: Tkinter is the inbuilt python module that is used to create GUI applications. It is one of the most commonly used modules for creating GUI applications in Python as it is simple and easy to work with.

SQL: Structured Query Language is a computer language that we use to interact with a relational database. SQL is a tool for organizing, managing, and retrieving archived data from a computer database.

Cryptography: In cryptography, encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information.

Hashing: Hashing is the practice of transforming a given key or string of characters into another value for the purpose of security. Although the terms “hashing” and “encryption” may be used interchangeably, hashing is always used for the purposes of one-way encryption, and hashed values are very difficult to decode.

I remain committed to my professional growth for which I have taken training courses specific to the skills in which I acknowledge a need for improvement.