

Industrial Internship Report on

Password Manager

Prepared by

Subhankar Mondal

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.

My project was a password manager, designed to provide a secure and efficient solution for managing passwords. It incorporated advanced encryption techniques to safeguard sensitive information, along with features such as random password generation. The project aimed to enhance user experience and promote secure password practices for improved security.

This internship gave me a very good opportunity to get exposure to Industrial problems and design/implement solutions for them. It was an overall great experience to have this internship.

TABLE OF CONTENTS

1	Preface	3
2	Introduction	5
2.1	About UniConverge Technologies Pvt Ltd.....	5
2.2	About upskill Campus	9
2.3	Objective	11
2.4	Reference	11
2.5	Glossary.....	11
3	Problem Statement.....	12
4	Existing and Proposed solution	13
5	Proposed Design/ Model	14
5.1	High Level Diagram (if applicable)	Error! Bookmark not defined.
5.2	Low Level Diagram (if applicable)	Error! Bookmark not defined.
5.3	Interfaces (if applicable).....	Error! Bookmark not defined.
6	Performance Test	15
6.1	Test Plan/ Test Cases	16
6.2	Test Procedure.....	16
6.3	Performance Outcome.....	17
7	My learnings.....	19
8	Future work scope	21

1 Preface

Summary of the 6 Weeks Password Manager Project Work

During the initial weeks, I conducted thorough research on encryption algorithms to determine the most suitable option for secure password encryption.

In the following weeks, I researched and implemented the necessary encryption algorithms, such as SHA-256, to ensure the passwords are securely encrypted. I also integrated hashing techniques to further enhance the security of stored passwords.

And finally, in the final weeks, I worked on designing and implementing the user interface using Tkinter. I created a user-friendly environment that allows users to easily store, retrieve, and manage their passwords for various accounts. Additionally, I added users to generate strong and unique passwords for their accounts.

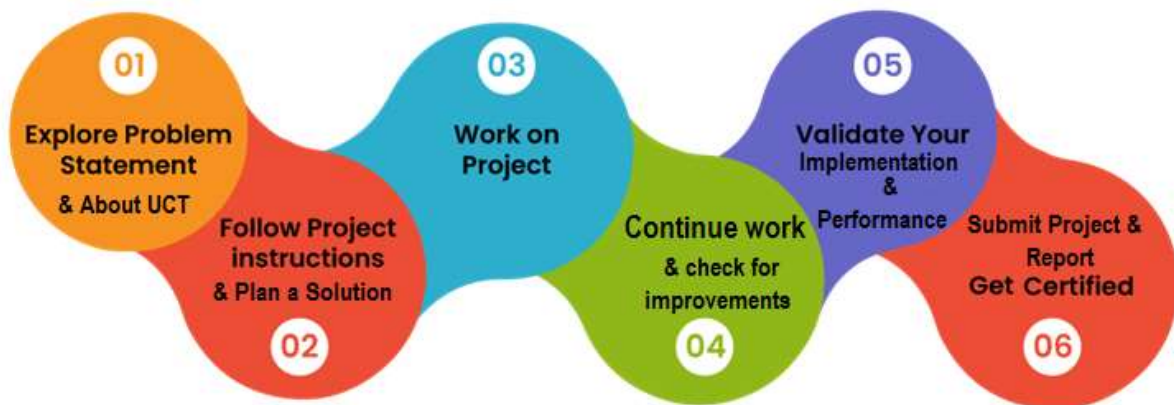
Relevant Internships provide a unique platform for skill development, allowing individuals to learn new technologies, tools, and methodologies that are directly applicable to the industry. This practical experience not only enhances their skill set but also demonstrates their ability to effectively apply their knowledge to solve real-world challenges. Moreover, internships offer insights into specific industries, exposing individuals to the inner workings of organizations and providing a deeper understanding of the industry's dynamics and demands.

My project is a password manager implemented using Python. In this project, I store a master password as a secret key in an encrypted format within a database. By providing the correct master key, users can access their password vault. Also, the master password can be retrieved by providing the correct recovery key. The vault serves as a secure storage for all the user's account details and information, which can be retrieved or updated as needed and also you can copy your existing password.

I am grateful for the valuable opportunity provided by USC/UCT and Upskills mentors, which allowed me to gain extensive knowledge about Python in just a few weeks. Working alongside experienced mentors enabled me to enhance my skills and dive deeper into the project. This experience has significantly strengthened my understanding of Python and I have learned a multitude of new concepts. I feel blessed to have this opportunity, as it has been instrumental in my personal and professional development.

The program was meticulously planned over a period of 6 weeks, encompassing a wide range of essential concepts to learn and master. Through this focused and well-structured approach, I was able to

significantly enhance my knowledge within a relatively short timeframe. The comprehensive nature of the program allowed me to delve into various important topics, gaining valuable insights and practical experience. This intensive learning experience has been instrumental in expanding my knowledge and skills effectively.



This internship has been an excellent learning opportunity for me. Throughout the duration of this program, I was able to enhance my knowledge and skills in areas such as Tkinter and encryption algorithms. The internship journey was not without its challenges, but I persevered and overcame each obstacle along the way. Overall, this internship has provided me with valuable hands-on experience and has greatly contributed to my personal and professional growth.

Thanks to all the Upskills Mentors who helped me directly or indirectly.

To my juniors and peers, I would like to share an important message: No matter the challenges you encounter during your work, never lose hope. With hard work and consistency, you can overcome any obstacle. Each problem you face is an opportunity to learn and grow. A valuable internship experience not only opens doors to new opportunities but also leaves a positive impression during interviews.

2 Introduction

2.1 About UniConverge Technologies Pvt Ltd

A company established in 2013 and working in the Digital Transformation domain and providing Industrial solutions with a 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.



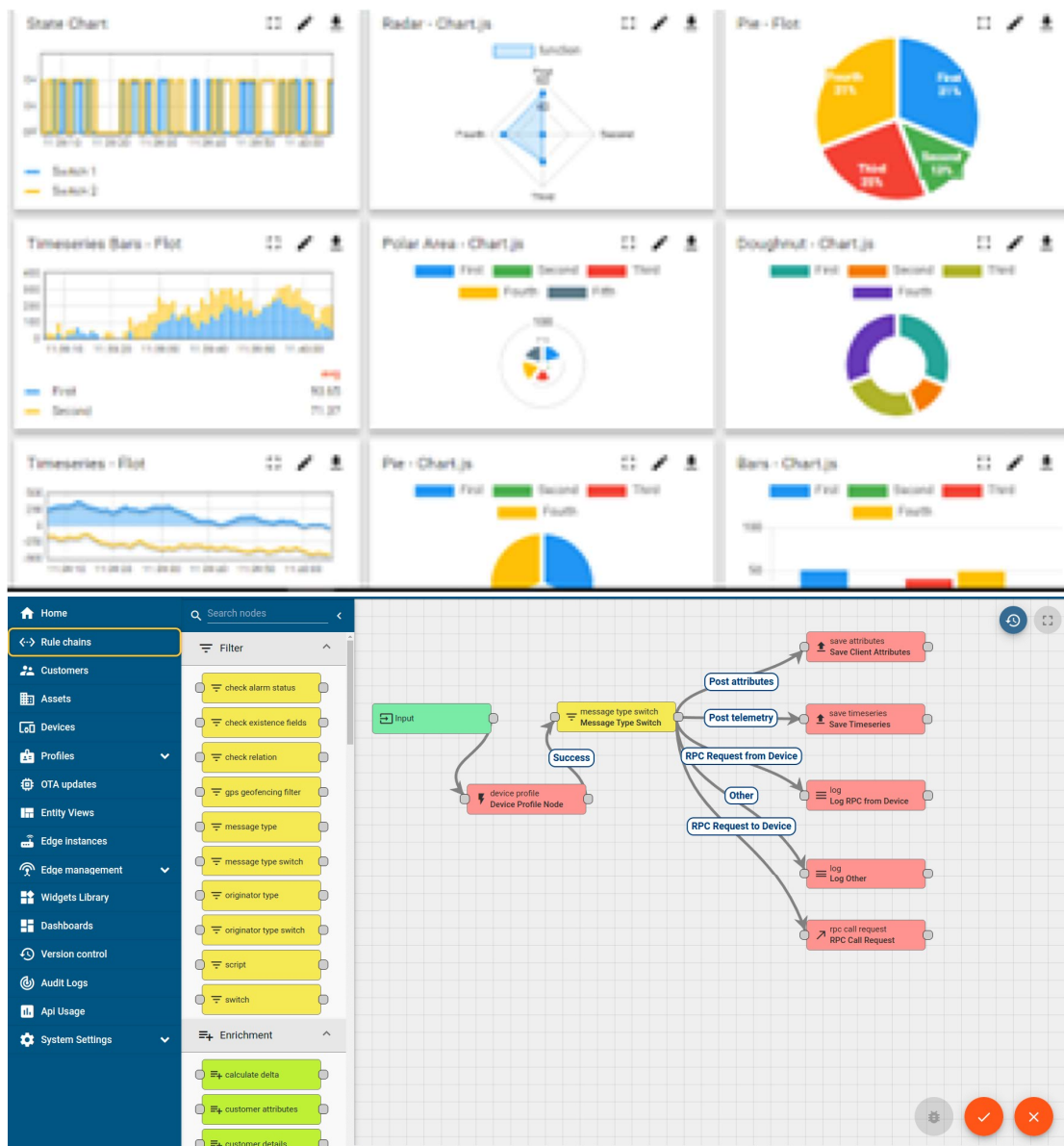
i. UCT IoT Platform ()

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 the backend and ReactJS for the 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 dashboard
- Analytics and Reporting
- Alert and Notification
- Integration with third party application(Power BI, SAP, ERP)
- Rule Engine



FACTORY WATCH

ii. Smart Factory Platform ()

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 unleash the true potential of the data that their machines are generating and help to identify the KPIs and also improve them.
- A modular architecture that allows users to choose the service that they want 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



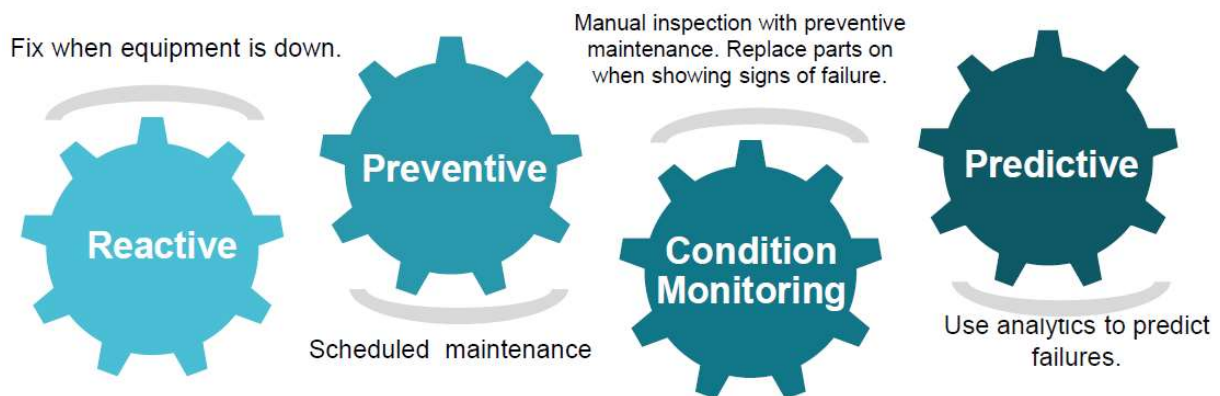


iii. LoRaWAN based Solution

UCT is one of the early adopters of Lora WAN technology and provides solutions in Agritech, Smart Cities, Industrial Monitoring, Smart Street lights, Smart Water/ Gas/ Electricity metering solutions etc.

iv. Predictive Maintenance

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

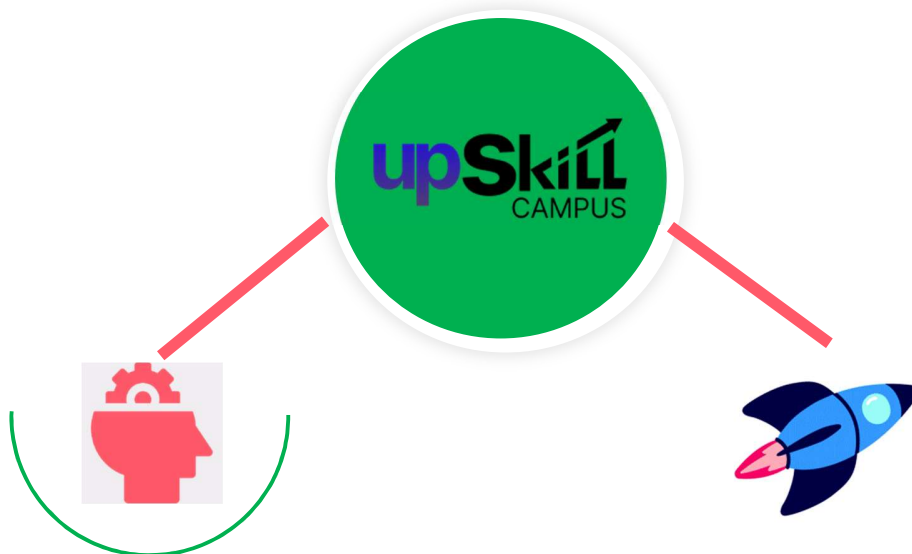


2.2 About upskill Campus (USC)

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.

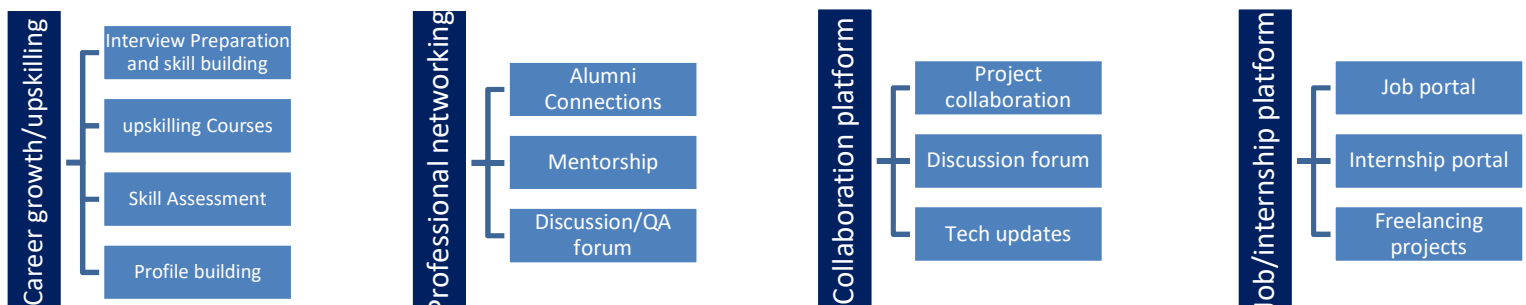




Seeing the need for upskilling in a self-paced manner along with additional support services e.g. Internships, projects, interaction with Industry experts, and Career Growth Services.

upSkill Campus aims to upskill 1 million learners in the next 5 years.

<https://www.upskillcampus.com/>



2.3 The IoT Academy

The IoT academy is EdTethe ch 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 of this internship program was to

- get practical experience working in the industry.
- to solve real-world problems.
- to have improved job prospects.
- to have an Improved understanding of our field and its applications.
- to have Personal growth like better communication and problem-solving.

2.5 Reference

- [1] W3Schools : [Python Functions \(w3schools.com\)](https://www.w3schools.com/python/python_functions.asp)
- [2] StackOverflow: [Stack Overflow - Where Developers Learn, Share, & Build Careers](https://stackoverflow.com/)
- [3] Tutorials point: Python-GUI programming (Tkinter)

2.6 Glossary

Terms	Acronym
Master Password	The primary password is set by the user to access the password manager vault.
Encryption/Decryption	The process of converting data into a secure and unreadable format using encryption algorithms to protect it from unauthorized access and vice versa for decryption.
SHA-256	A cryptographic hash function from the Secure Hash Algorithm family is widely used for data integrity and security.
Recovery Key	A randomly generated string is provided to the user during the registration process used for password recovery in case the master password is forgotten.
Hashing	A one-way process of converting data into a fixed-length string of characters using a hash function, commonly used to securely store passwords.

3 Problem Statement

In the assigned problem statement

- **Password Manager:**

The problem statement for the password manager project is to create a secure and convenient solution for managing user passwords. Users often struggle with remembering multiple passwords for different accounts, leading to weak passwords or reusing the same password. This poses a significant security risk. The password manager aims to address this challenge by securely storing and organizing passwords, generating strong and unique passwords, and providing a reliable method to retrieve passwords when needed. The goal is to enhance password security, reduce the risk of data breaches, and simplify the password management process for users.

4 Existing and Proposed solution

Summary of existing solutions provided by others and their limitations:

Even though there are solutions already in place, it is important to note that some of them incorrectly implement the master password and others cannot produce a random recovery key. The password management system's complete authentication and security are compromised by the lack of these elements, which reduces their ability to guarantee reliable data protection and user authentication.

Furthermore, it's crucial to emphasize that several of the current solutions lack user-friendliness in terms of their aesthetic appeal and general design. The aesthetics and simple user interface significantly contribute to improving the user experience and making the password management solution more approachable and practical for users.

My Proposed Solutions:

My solution involves implementing a more secure and robust master password mechanism, ensuring enhanced authentication. Additionally, I have prioritized creating a user-friendly environment, focusing on intuitive design and a visually appealing interface. By combining these aspects, my solution aims to provide a comprehensive and user-centric password management experience.

My Value addition I am planning:

I am planning to add value by incorporating features such as advanced encryption algorithms, and user-friendly behavior. By continuously enhancing security and usability, my goal is to provide a comprehensive and user-friendly password management solution with added value.

4.1 Code submission (GitHub link):

<https://github.com/subhankar74/upskillcampus>

4.2 Report submission (GitHub link):

<https://github.com/subhankar74/upskillcampus>

5 Proposed Design/ Model

My proposed Model is a popup application built on the base of TKinter, and encryption algorithms, and utilizes SQLite3 as the database. The model follows a secure process for user sign-up and access to the application. During the initial sign-up, users are required to set their master password, which serves as the primary password for accessing the vault or the application. Additionally, a random recovery key is generated and securely stored for future recovery or reset purposes. This recovery key becomes essential if a user forgets their master password, as it enables them to regain access to the application.

When a user opens the application for the second time, they only need to provide their master password. However, if a user forgets their master key, they can initiate the recovery or reset procedure. By providing the correct recovery key, users can create a new master key and successfully log in to the application again. This two-step process ensures both security and accessibility for users, as they can securely store and retrieve their passwords while having a fail-safe mechanism in place for password recovery.

After successfully logging in, users can access their vault data and add new entries by clicking the text boxes of each website name, username and password then users have to click the save button to save these data. This action triggers a popup window where users can enter the required information for the new entry. They have the option to manually enter their password. In addition to adding new data, users have the flexibility to manage their existing entries. They can easily delete any unwanted data or update the information as needed and the user can copy the password, by clicking the copy password button for using it to log in to desire sites. This allows users to maintain an organized and up-to-date vault, ensuring efficient password management.

The design strategy focuses on preserving the integrity and confidentiality of user data through the use of powerful encryption algorithms and secure storage techniques. By combining the user-friendly interface of TKinter, the robustness of encryption algorithms, and the reliability of SQLite3 as the database, the application provides a secure and efficient password management solution for users.

6 Performance Test

The password manager project holds significant value for real industries rather than just being an academic project:

In today's digital age, cybersecurity is a critical concern for industries of all types. Data breaches, identity theft, and unauthorized access to sensitive information are real risks that businesses face. By developing a robust password manager, real industries can enhance their security measures and protect their employees' and customers' sensitive data. Also, Industries often deal with a large number of accounts and passwords across various platforms and systems. A password manager streamlines the process of password management, enabling employees to securely store, generate, and access their passwords. This increases productivity and reduces the risks associated with weak or reused passwords.

For my password manager project, several constraints need to be considered, here are some important ones:

Security: Ensuring strong security measures is the main restriction for a password manager. To protect private user information, it should use powerful encryption algorithms.

Usability and User Experience: The interface of the password manager should be simple and easy to use. It should be simple to use. Also, Password addition, retrieval, and updating ought to be simple and quick processes.

And I overcome those constraints by following these steps:

For Security, I've used the SHA-256 encryption algorithm and hashing techniques for strong data encryption to increase security. This adds a layer of security by guaranteeing that the data is encrypted in a highly secure and encrypted manner.

And for user Experience, I added the ttk module and made use of colourful, eye-catching design elements to improve user experience. By making these changes, we hope to create a user-friendly interface that effortlessly leads users through the application and enhances their enjoyment of it.

6.1 Test Plan/ Test Cases

A user's master password is encrypted and hashed when they register for the first time, then it is saved in a SQLite3 database for future logins. The password's security is ensured by this procedure.

The user only needs to enter the master password for subsequent logins. The system then compares the stored hashed password to the input hash after retrieving it from the database. The user is given access to their account if they match.

Additionally, for enhanced security, the user's information is also encrypted before being stored in the database. This encryption process ensures that sensitive user data, such as personal details or any other confidential information, is protected from unauthorized access.

6.2 Test Procedure

Firstly, I converted the data from its original string format into Unicode characters. Then, I translated these characters into a string of binary digits. This binary representation was then passed through an encryption algorithm, followed by a hashing process, to securely encrypt the master password.

During the user login process, the provided master password by the user undergoes the same procedure of conversion into Unicode characters, followed by a translation into a binary string. This binary representation is then processed through the encryption algorithm and hashing process, resulting in a final encrypted format. The encrypted master password is then checked against the stored encrypted password to determine if they match. If the encrypted passwords match, the user is granted access to proceed further.

In the vault screen, users can add data by clicking the Save button and providing all the necessary user information, including a generated password. The data is then encrypted using the encryption algorithm and securely stored in the database.

```
kdf = PBKDF2HMAC(  
    algorithm=hashes.SHA256(),  
    length=32,  
    salt=salt,  
    iterations=100000,  
    backend=backend  
)  
encryptionKey = 0
```

6.3 Performance Outcome

Sign-up Phase: The users start by entering the master password and they have to re-enter the master password for clarifying that they have entered their desired password correctly.

As an additional security measure, a recovery key is generated during the encryption process. This recovery key serves as a means to recover the master password in case it is forgotten. So users have to store this recovery key safely and not show anyone or not share it with anyone, otherwise who knows this recovery key can change the user master key and they can use the user's password vault with bad intentions.

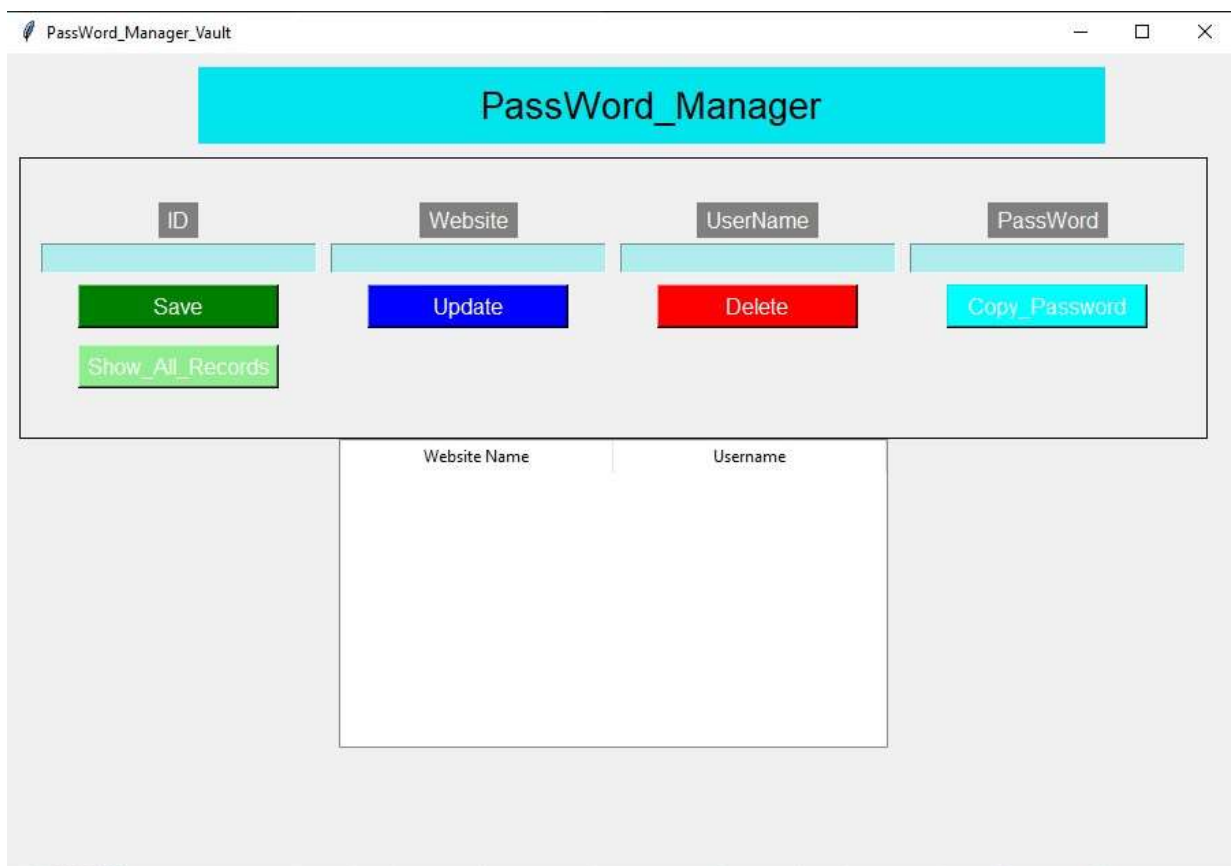


When users press the Done button then they can enter the password vault successfully.

Login Phase: During the login procedure, if the user is already registered, they will only be prompted to enter their master password. However, if the user forgets their master password or wants to change the existing master password, they can go through the recovery procedure to change the master password and regain access to their account.

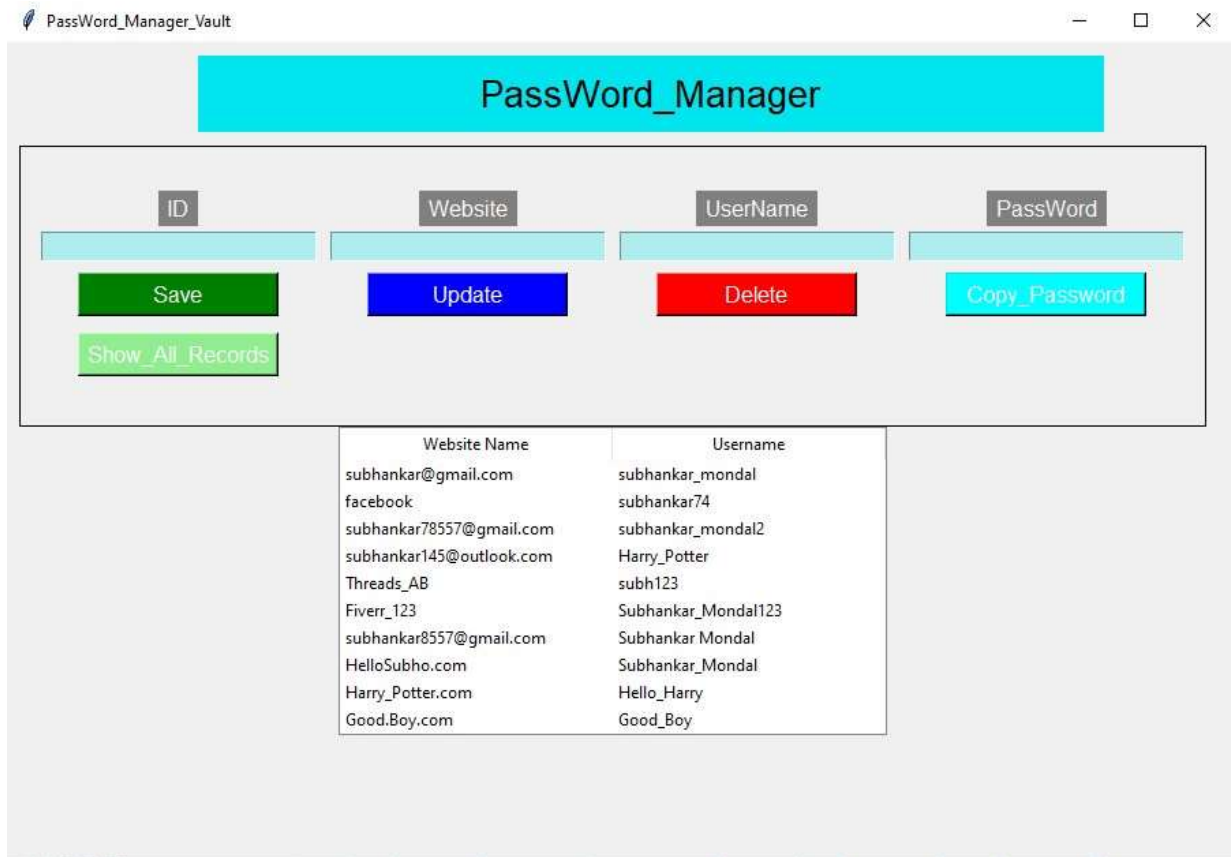



Vault Page: Users can examine their current data on the vault page and have the ability to add more data by clicking the text boxes of the website name, username and password. Then they have to click the 'Save' button to save this data on the password vault. Users can also erase data by clicking the 'Delete' button or update current data by clicking the 'Update' button. Users can copy the particular password by clicking the 'Copy_Password' button for using that password to log in to the mentioned website.



ID	Website	UserName	PassWord

And users can see all the recorded data by clicking the 'Show_All_Records' button and there only the website name and the username are shown.



7 My learnings

Learning about Encryption: By Exploring encryption algorithms I enhanced my understanding of its capabilities, data security, and protection against breaches and harvesting. Also Applying encryption techniques in the password manager ensures robust data security and safeguards against unauthorized access.

Learning about Tkinter: I gained knowledge about interactive user interface design and feature implementation with the Tkinter Python library. This enhanced the usability of the program and the user experience.

Learning About Sqlite3: I also learned how to utilize the sqlite3 a Python MySQL module to securely store and retrieve encrypted data in a database. This allowed for efficient data management and decryption when required.

Learning about User Experience: I also explored different modules of Tkinter, such as TTK, to enhance the user experience by creating visually appealing and interactive interfaces. This allowed for a more engaging and user-friendly application.

8 Future work scope

The Password Manager project's future scope includes a number of potential improvements and expansions. Future development may occur in some of the following areas:

Multi-factor authentication: Adding extra layers of protection to user accounts, such as OTP (one-time password) verification or mail verification.

Password strength analysis: Implementing a feature that evaluates the strength and complexity of user-generated passwords and makes security-enhancing recommendations.

Cross-platform compatibility: Adapting the programme to work with other platforms, such as mobile, and online platforms, devices etc.

Asking for master key: When the user wants to copy the password of a particular website from the password vault. Then users have to give the master key to the copy_password window. Only Then the user can copy the password. Because in the password vault, only the website name and username are shown so without knowing the master key no one access or copy the password of a particular website. It will enhance security.