**Industrial Internship Report on**

**Password manager**

**Prepared by**

**POLIMI BHANU PRAKASH**

|  |
| --- |
| *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 “.  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 3](#_Toc139702806)

[2 Introduction 4](#_Toc139702807)

[2.1 About UniConverge Technologies Pvt Ltd 4](#_Toc139702808)

[2.2 About upskill Campus 8](#_Toc139702809)

[2.3 Objective 9](#_Toc139702810)

[2.4 Reference 9](#_Toc139702811)

[2.5 Glossary 10](#_Toc139702812)

[3 Problem Statement 11](#_Toc139702813)

[4 Existing and Proposed solution 12](#_Toc139702814)

[5 Proposed Design/ Model 13](#_Toc139702815)

[5.1 High Level Diagram (if applicable) 13](#_Toc139702816)

[5.2 Low Level Diagram (if applicable) 13](#_Toc139702817)

[5.3 Interfaces (if applicable) 13](#_Toc139702818)

[6 Performance Test 14](#_Toc139702819)

[6.1 Test Plan/ Test Cases 14](#_Toc139702820)

[6.2 Test Procedure 14](#_Toc139702821)

[6.3 Performance Outcome 14](#_Toc139702822)

[7 My learnings 15](#_Toc139702823)

[8 Future work scope 16](#_Toc139702824)

# Preface

A password manager is a software application that is used to store and manage the passwords that a user has for various online accounts and security features. Password managers store the passwords in an encrypted format and provide secure access to all the password information with the help of a master password.

Password managers enable the use of strong and unique passwords for each online account and provide an efficient way to manage all the passwords. The login information is encrypted and stored in either the local memory of the user’s system or in cloud storage. Portable password manager applications installed in mobile devices can also be used as a way to manage and remember passwords anywhere and use them on shared systems.

 Chrome, Firefox, and Safari are each able to store passwords once you create them, right from a website, and then give you that information back when it's needed for a login form. Many of the password manager applications and all of the browser-based ones offer the ability to synchronize your saved passwords to other computers where you've signed in. You can decide whether to enable this feature or not and if you have more than one computer, or a computer and a mobile device where you use passwords, it can be very helpful. As you can see, these tools make it much easier to work with strong passwords and reduce the burden of keeping separate passwords for different sites. But not everyone is comfortable with storing their passwords electronically or syncing them to the cloud. If you're not comfortable using software to track your passwords, you can use a paper notebook to hold them, as long as you keep that notebook away from prying eyes. A software solution is generally much more secure, but some people aren't comfortable with using software password managers. Keep your notebook in a safe, or in a locking drawer in your desk. Don't use a sticky note or something that's easy to leave out or to lose, and make sure to leave space to write in a new password if you change a password, as you should every now and then. It used to be common wisdom to never write down passwords, but that practice led to people making their passwords short or simple in order to better remember them, and in the modern world of the Internet, a simple or short password is not sufficient to protect an account. As I mentioned earlier, setting a strong password that's unique to each site you use is much more important. Using a different password for each site can be daunting, but with password management tools, we can make it a lot easier.

Thankyou to the friends who helped me in this project(Navya,Lakshmi,Vasanth)

Dear juniors and peers,

As I reflect on my internship experience and the knowledge I have gained in forecasting “password manager”, I want to share a message with all of you.

Firstly, embrace the opportunity to work in the field of python and its applications in solving real-world challenges. The world is increasingly relying on data-driven approaches to make informed decisions, and password manager in smart cities is just one example. The insights we can derive from data have the power to shape the future and make a meaningful impact on people's safety.

Secondly, be curious and eager to learn. python is a rapidly evolving field, and there is always something new to explore and discover. Take advantage of the resources available to you, whether it's online courses, research papers, or collaboration with peers. Continuously update your skills and stay abreast of the latest developments in data science methodologies and tools.

Additionally, embrace teamwork and collaboration. Solving complex challenges requires diverse perspectives and expertise. Engage with your peers, share ideas, and learn from each other's experiences. Collaborative projects not only enhance your learning but also foster creativity and innovation.

Lastly, approach every project with enthusiasm and a growth mindset. Each opportunity, whether it's an internship or a classroom assignment, is a chance to expand your knowledge, sharpen your skills, and contribute to meaningful solutions. Embrace challenges, persevere through setbacks, and celebrate your achievements along the way.

Remember, the field of python is full of possibilities. As the world continues to advance towards smarter cities and intelligent systems, we have the chance to be at the forefront of this transformation. So, let's make the most of our skills, passion, and knowledge to create a positive impact on society.

Best wishes for your future endeavors!

Sincerely,

**POLIMI BHANU PRAKASH**

# Introduction

## 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.



1. 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

 

1. **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 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.

 

1.  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.

1. 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.



## 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

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

upSkill Campus aiming to upskill 1 million learners in next 5 year



## 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.

## 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.

## Reference

[1]."Cryptography Engineering: Design Principles and Practical Applications" by Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno: This book covers the principles and practices of cryptography, including encryption algorithms and protocols used in password management systems.

[2]."Security Engineering: A Guide to Building Dependable Distributed Systems" by Ross Anderson: This comprehensive book discusses various aspects of security engineering, including authentication, access control, and secure storage, which are relevant to password managers.

[3]."Perfect Passwords: Selection, Protection, Authentication" by Mark Burnett: This book explores the concepts of password security, offering insights into creating strong passwords, managing passwords effectively, and protecting against password-related risks.

## Glossary

|  |  |
| --- | --- |
| Terms | Acronym |
| Resource | Denotes the server/application/device whose user accounts and passwords are to be managed by Password Manager Pro. |
| Resource Group | Denotes the group to which a particular resource belongs. For example, if you have some Windows XP servers among a number of other windows servers, you can group all the XP servers as one resource group. |
| User | Denotes the Password Manager Pro user accounts created as part of Password Manager Pro User Management |
| User Group | Group of Password Manager Pro Users. |
| Agent | Password Manager Pro utilizes an agent for establishing connections with the remote resources. |

**3 Problem Statement**

Most users recycle their passwords across numerous websites and choose very weak passwords. How are you expected to create secure, one-of-a-kind passwords for every website you visit? A password manager offers the answer.

The purpose of a password manager is to safely store online credentials, help you log in into any account automatically and generate strong and unique passwords. A master password is used to lock down an encrypted vault where these passwords are kept.

A password manager is a computer program that allows users to store and manage their passwords for local applications or online services such as web applications, online shops or social media.

Password managers can generate passwords[3] and fill online forms. Password managers may exist as a mix of: computer applications, mobile applications, or as web browser extensions.

A password manager may assist in generating passwords, storing passwords, usually in an encrypted database.Aside from passwords, these applications may also store data such as credit card information, addresses, and frequent flyer information.

The main purpose of password managers is to alleviate a cyber-security phenomenon known as password fatigue, where an end-user can become overwhelmed from remembering multiple passwords for multiple services and which password is used for what service.

Password managers typically require a user to create and remember one "master" password to unlock and access all information stored in the application. Password managers may choose to integrate multi-factor authentication. through fingerprints, or through facial recognition software.Although, this is not required to use the application/browser extension.

Password managers may be installed on a computer or mobile device as an application or as a browser extension.

# Existing and Proposed solution

Existing solution

There are several existing solutions for password managers that are widely used and trusted by individuals and organizations. Here are some popular options:

LastPass: LastPass is a cloud-based password manager that securely stores your passwords and other sensitive information. It offers browser extensions, mobile apps, and multi-factor authentication options for added security.

1Password: 1Password is a password manager that stores your passwords, credit card information, and other important data in a secure vault. It provides browser extensions, mobile apps, and supports multi-factor authentication.

Dashlane: Dashlane is a user-friendly password manager that allows you to store passwords, generate strong passwords, and autofill forms on websites. It offers secure syncing across multiple devices, biometric authentication, and a built-in VPN for added privacy.

KeePass: KeePass is an open-source password manager that allows you to store passwords in an encrypted database. It offers a range of features including password generation, auto-typing, and plugin support. KeePass databases can be synced across devices using third-party cloud storage services.

Bitwarden: Bitwarden is an open-source password manager that offers free and premium plans. It provides strong encryption for storing passwords, supports various platforms and browsers, and offers two-factor authentication.

NordPass: NordPass is a password manager developed by the creators of NordVPN. It provides a secure vault for storing passwords, supports multiple devices, and includes features like password generation and password sharing.

## Code submission (Github link):

<https://github.com/polimibhanuprakash/upskill_campus/tree/main/CODE%20%26%20REQUIREMENTS>

## Report submission (Github link) :

<https://github.com/polimibhanuprakash/upskill_campus>

# Proposed Design/ Model

This is simple Password Management System graphical user interface developed using visual Basic. It allows the user to add account information for different accounts he holds on the internet. Password Management System basically stores the user name and password details in an encrypted format in the database. The encryption is managed by blow fish algorithm. The user has to login to the system. It checks for the validity of the user. The user shall be able to add account. The user can add user name and password details and save to the database. The list of accounts held by the user is displayed on the left screen. When the user selects the particular account on the left panel, the details of the account gets displayed on the right screen. The password shall be displayed in encrypted format. Once the user selects un hide option, he shall be able to view the password on screen. The user can add any number of accounts using this application. The encryption algorithm is very robust and uses the symmetric key block cipher which is very effective way of handling passwords.

System Specifications

Password Management System Modules

User details: This module shall have the details of the user. It holds the user name and password details to the interface.

Account password Module: This module will have the details regarding the different accounts held by the user over the internet. It holds information about different account names, user names and passwords. These passwords are stored in encrypted format.

**Hardware configuration**

Intel dual core

512 MB Ram

Hard disk 80 GB

Key board Standard

**Software configuration**

Operating system Windows 7

Language Visual Basic 6.0

Blow fish Encryption Algorithm

# Performance Test

## Test Plan/ Test Cases

1. Test Objective
2. Test Scope
3. Test Environment
4. Test Approach
5. Test Schedule
6. Test Resource
7. Test Deliverables
8. Test Risks and Mitigation

## Test Procedure

Testing and quality assurance are crucial aspects of a password management project to ensure

its reliability, security, and user-friendliness. Here are some key considerations:

1. Unit testing: Test individual components of the password management system, such as

password encryption, storage, and retrieval, to verify their functionality and correctness.

2. Integration testing: Test the integration of various modules and components within the

password management system to ensure they work together seamlessly.

3. Security testing: Conduct penetration testing and vulnerability assessments to identify any

potential security weaknesses or vulnerabilities in the system.

4. Performance testing: Evaluate the performance and responsiveness of the password

management system under different loads and stress conditions to ensure it can handle a large

number of users and transactions without performance degradation.

5. Usability testing: Test the user interface and user experience of the password management

system to ensure it is intuitive, user-friendly, and meets the needs of the target users.

6. Compatibility testing: Verify that the password management system is compatible with

different operating systems, browsers, and devices commonly used by the target users.

7. Regression testing: Perform regression tests to ensure that any updates or changes to the

password management system do not introduce new bugs or issues and do not impact existing

functionality.

8. Accessibility testing: Evaluate the accessibility of the password management system to

ensure it can be used by individuals with disabilities, adhering to accessibility standards and

guidelines.

9. Error handling and recovery testing: Test the system's ability to handle errors, recover from

failures, and gracefully handle exceptional scenarios such as password resets, account

lockouts, or system crashes.

10. Compliance testing: Verify that the password management system complies with relevant

security and privacy regulations, such as encryption standards, data protection laws, and

industry-specific compliance requirements.

By implementing comprehensive testing and quality assurance measures, organisations can

minimise the risks associated with password management projects, enhance the security.

## Performance Outcome

The performance outcome of a password manager project can be measured based on various factors. Here are some key performance outcomes that can be considered:

Security: One of the primary objectives of a password manager is to enhance security. The performance outcome in this regard can be measured by assessing the effectiveness of the encryption algorithms used, the strength of the generated passwords, and the overall security measures implemented. A positive performance outcome would indicate a robust and reliable security system, capable of protecting user passwords from unauthorized access.

User-Friendliness: The performance outcome of a password manager project can also be evaluated based on its user-friendliness. This includes the ease of use, intuitiveness of the user interface, and the overall user experience. Positive performance outcomes in this area would indicate that users find the password manager convenient, accessible, and easy to navigate.

Compatibility: The performance outcome of a password manager project can also be assessed based on its compatibility with various platforms and devices. A positive outcome would indicate that the password manager works smoothly across different operating systems, browsers, and mobile devices, ensuring seamless access to stored passwords regardless of the user's preferred technology.

Integration: The ability of a password manager to integrate with other applications and services can also be a performance outcome. Integration with web browsers, operating systems, or other password-related services can enhance the overall user experience. Positive performance outcomes in this regard would indicate seamless integration with popular software and services, allowing users to conveniently utilize the password manager across multiple platforms.

Password Management Capabilities: The performance outcome can also be measured by evaluating the core functionalities of the password manager. This includes features such as password generation, password autofill, secure password sharing, and password change notifications. Positive performance outcomes would indicate that these functionalities are reliable, efficient, and meet the needs of users effectively.

Reliability and Stability: The performance outcome of a password manager project can be assessed based on its reliability and stability. This includes factors such as the absence of bugs, crashes, or data loss issues. Positive outcomes in this area would indicate that the password manager operates consistently without interruptions or significant technical issues.

# My learnings

Working on a password manager project can provide valuable insights and learnings in various aspects. Here are some common learnings you might have gained during your project:

Security Principles: Developing a password manager requires a deep understanding of security principles and best practices. You likely learned about encryption, hashing, salting, and other techniques to protect user passwords and sensitive information.

User Authentication: Implementing secure user authentication is crucial for a password manager. You may have learned about various authentication methods, such as username/password, biometric authentication (fingerprint or face recognition), two-factor authentication (2FA), or multi-factor authentication (MFA).

Encryption Algorithms: Understanding encryption algorithms is essential for securing passwords and sensitive data. You might have explored different algorithms like AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman) and their appropriate usage in the context of a password manager.

Database Management: A password manager typically requires a database to store user credentials securely. You likely learned about database management concepts, such as designing schemas, implementing CRUD (Create, Read, Update, Delete) operations, and optimizing query performance.

Password Generation: Implementing a password generator is a common feature in password managers. You might have explored various password generation techniques, including password length, complexity rules, and randomness, to provide strong and unique passwords for users.

Error Handling and Security Vulnerabilities: During the development process, you may have encountered various errors, bugs, and security vulnerabilities. Learning how to handle errors gracefully and addressing security issues, such as cross-site scripting (XSS), SQL injection, or session management vulnerabilities, can be invaluable.

User Feedback and Iterative Development: Throughout the project, you may have sought user feedback, conducted testing, and iteratively improved the password manager based on the insights gained. This iterative development process helps refine the product and ensures that it meets user requirements and expectations.

Remember that these learnings are general and may vary depending on the scope and specific requirements of your password manager project. It's important to continuously explore and stay updated on the latest security practices and technologies to ensure the ongoing security and functionality of your application.

# Future work scope

While working on the project of forecasting traffic patterns in smart cities, there may have been certain ideas or aspects that couldn't be explored fully due to time limitations. Here are some potential areas for future work and further enhancements to consider:

In the future, password managers are likely to evolve and incorporate several new features and enhancements to provide even better security and convenience for users. Here are some potential areas of future work scope for password managers:

Advanced authentication methods: Password managers may integrate additional authentication methods beyond master passwords, such as biometric authentication (fingerprint, facial recognition, etc.), hardware tokens, or multi-factor authentication (MFA). These methods can further enhance security and make it more difficult for unauthorized users to access sensitive information.

Password health and analysis: Password managers could include features that analyze the strength and security of stored passwords. This analysis could identify weak or compromised passwords, flag duplicated passwords used across multiple accounts, and suggest stronger alternatives. By actively monitoring password health, users can be better protected against potential security breaches.

Dark web monitoring: Password managers may integrate with dark web monitoring services to alert users if their credentials appear in known data breaches or if their personal information is at risk. This feature would enable users to take immediate action, such as changing compromised passwords or monitoring their accounts for suspicious activity.

Enhanced synchronization and cross-device support: Password managers are likely to improve their synchronization capabilities across multiple devices and platforms. This could involve seamless integration with various operating systems, browsers, and mobile devices, allowing users to access their passwords and secure information from anywhere, at any time.

Integration with identity management systems: Password managers could integrate with identity management systems to provide a comprehensive solution for managing not just passwords but also other aspects of digital identity. This integration could enable centralized control over user access, authentication policies, and privileges, making it easier to manage and secure multiple accounts.

****

**Submitted by:**

**POLIMI BHANU PRAKASH**

**Madanapalle Institute of Technology & Science(MITS)**

**Gmail:bp6108325@gmail.com**