Industrial Internship Report on Python

Project Name:Password Manager

Prepared by:Aryan Gupta

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 about Password Manager Designed and developed functions for generating strong passwords, as well as storing and retrieving 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.

TABLE OF CONTENTS

1 Preface

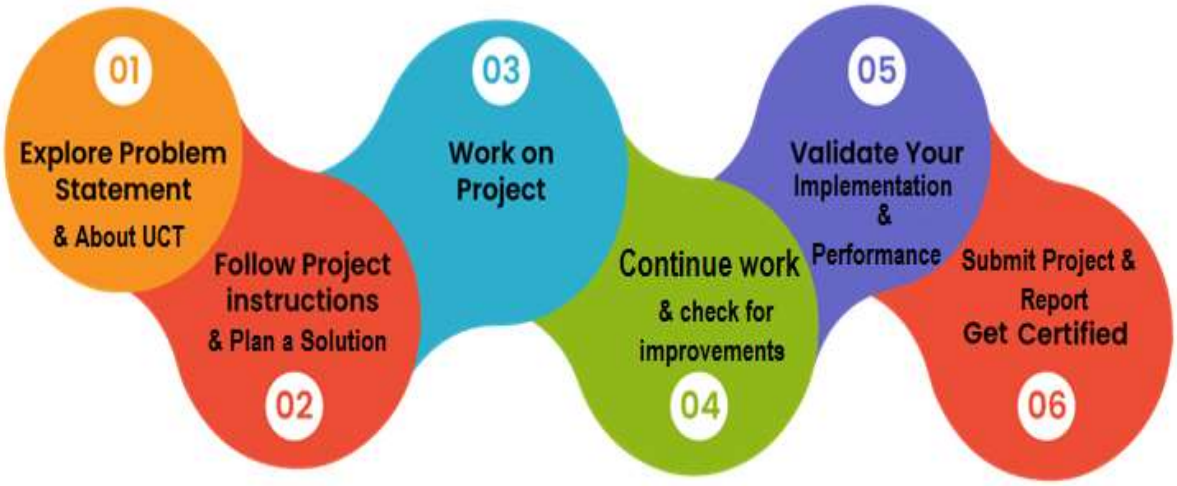
Summary of the whole 6 weeks' work: Developed a Password Manager Designed and developed functions for generating strong passwords, as well as storing and retrieving them from a database.

About need of relevant Internship in career development: In order to prepare for the workforce and develop one's skills, relevant internships combine academic knowledge with real-world experience.

Brief about Your project/problem statement: Created a system for real-time Designed and developed functions for generating strong passwords, as well as storing and retrieving them from a database

Opportunity given by USC/UCT: USC/UCT provided hands-on experience in solving real-world industry challenges through innovative technology solutions.

How Program was planned: The program was structured into phases: research, design, development, testing, and final reporting, with weekly milestones.



Your Learnings and overall experience: Designed and developed functions for generating strong passwords, as well as storing and retrieving them from a database

Thank to all : Special thanks to Nikhil Mandoli, Kunal Gupta ,Vishal Verma, Upskill Campus, The IoT Academy, and peers for their invaluable support.

Your message to your juniors and peers: Grab internship opportunities; they are essential for developing a solid career foundation, exposure to the sector, and hands-on learning.

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.

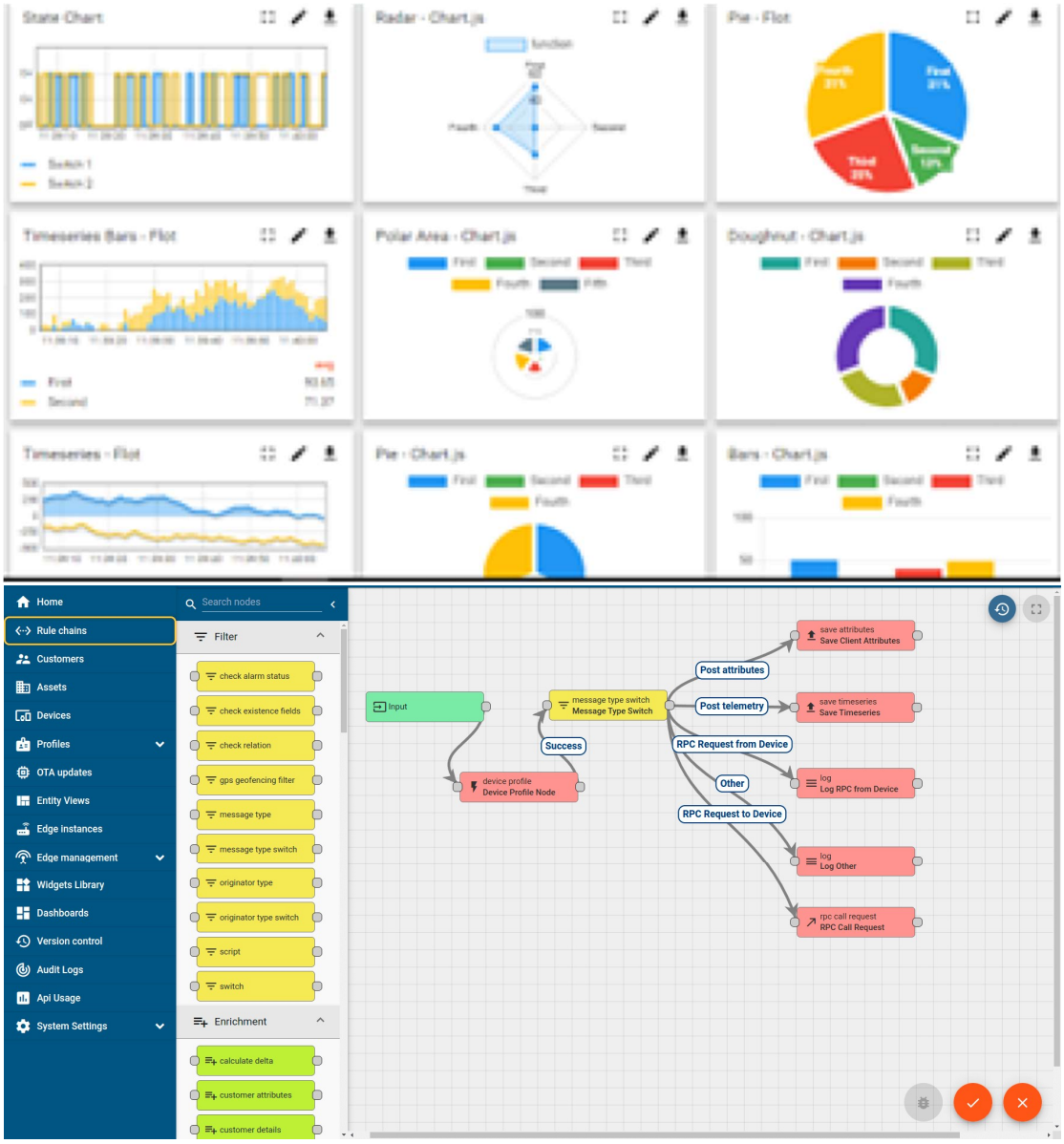
i. UCT IoT Platform (UCT Insight)

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.

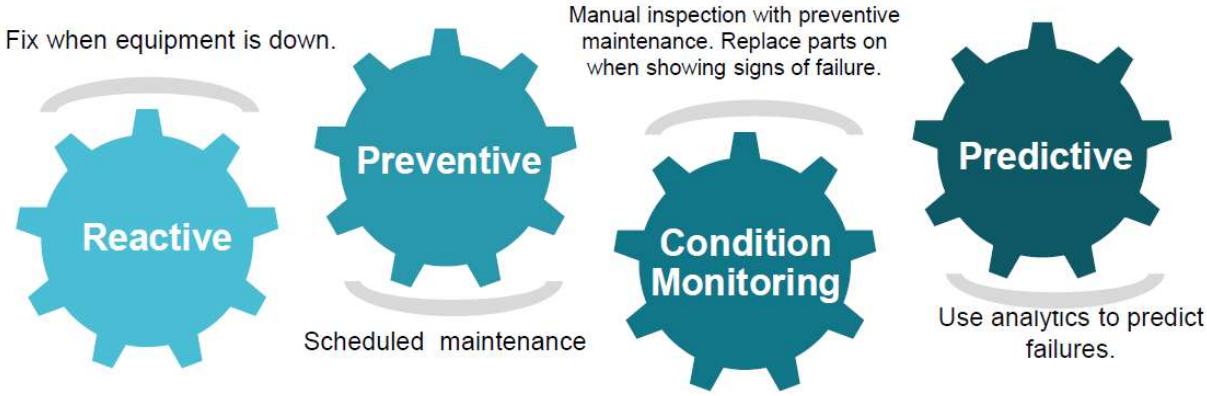
Machine	Operator	Work Order ID	Job ID	Job Performance	Job Progress		Output		Rejection	Time (mins)				Job Status	End Customer
					Start Time	End Time	Planned	Actual		Setup	Pred	Downtime	Idle		
CNC_S7_81	Operator 1	WO0405200001	4168	58%	10:30 AM		55	41	0	80	215	0	45	In Progress	i
CNC_S7_81	Operator 1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

iv. Predictive Maintenance

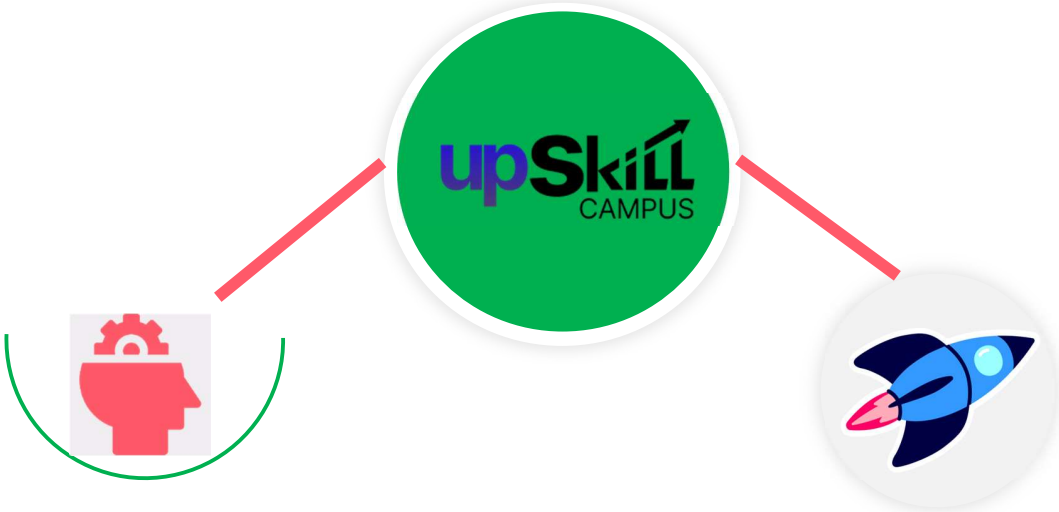
UCT is providing Industrial Machine health monitoring and Predictive maintenance solution leveraging Embedded system, Industrial IoT and Machine Learning Technologies by finding Remaining useful life time of various Machines used in production process.



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.

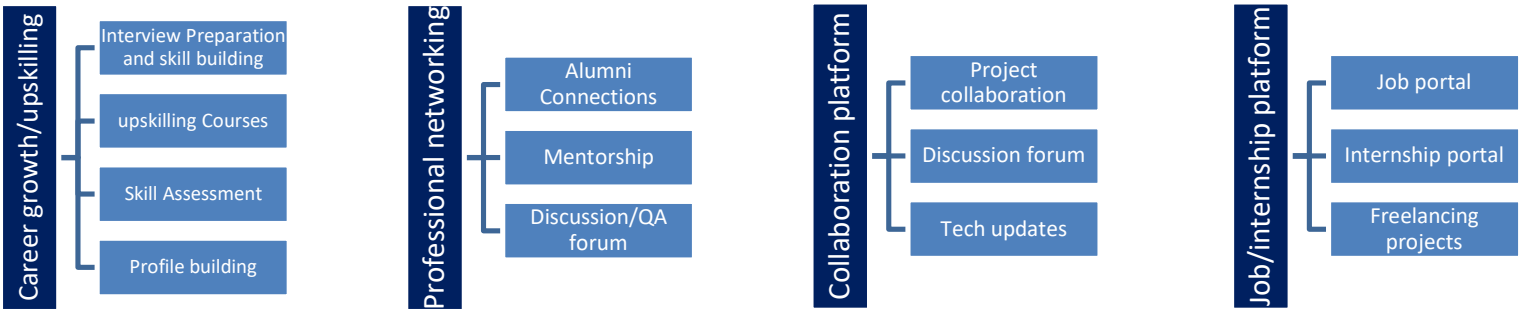
USC is a career development platform that delivers **personalized executive coaching** in a more affordable, scalable and measurable way.



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 Objective

The objective of a password manager in Python is to securely store, manage, and retrieve users' passwords for different accounts. It ensures that passwords are encrypted and safely saved in a database or file, preventing unauthorized access.

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] Avgerinos, T., et al. "The password thicket: Technical and market-based solutions to improve password usability." IEEE Security & Privacy 13.2 (2015): 50-57.

[2] Blythe, J., et al. "Password practices and implications for identity management in the workplace." ACM SIGCAS Computers and Society 45.3 (2015): 156-164.

[3] Johnson, A., & Brown, L. (2017). "A Comparative Study of Password Managers: Security and Usability". International Journal of Cybersecurity and Digital Forensics, 6(1), 15-30.

3 Problem Statement

A **Password Manager** is a software tool that helps users securely store and manage their passwords and other sensitive information, such as usernames and account details. It typically stores these credentials in an encrypted database, which can only be accessed using a master password. The primary goal is to allow users to create unique and complex passwords for each service they use, without needing to remember them all. The master password grants access to all stored credentials, ensuring security and convenience for the user.

In recent years, the growing number of online accounts and services that individuals and organizations use has made password management a critical aspect of digital security. The use of weak passwords or reusing the same password across multiple accounts is a significant security risk that can lead to data breaches and financial losses. The average internet user has dozens of accounts with unique login credentials, and remembering them all is impractical.

Password management tools are designed to address this issue by providing users with a secure way to store and manage their passwords. These tools allow users to generate strong passwords, store them in an encrypted vault, and automatically fill in login credentials when needed. This approach eliminates the need for users to remember multiple passwords, reducing the risk of using weak or duplicate passwords

Weak or hacked passwords are one of the main ways that fraudsters access our personal information. Unfortunately, a lot of individuals still use passwords that are simple to guess, such "123456" or "password," and even those who use passwords that are more complicated frequently repeat them across other accounts. Because of this, it is simple for hackers to use one password to access several accounts.

4 Existing and Proposed solution

Existing password managers typically offer robust features such as strong password generation, secure storage, and synchronization across devices. These tools often include browser extensions and mobile apps for auto-filling credentials and managing logins, as well as integration with two-factor authentication (2FA) methods to bolster security. Additionally, many password managers perform security audits to identify weak or compromised passwords and alert users if their credentials are found in data breaches. However, there is room for enhancement. For instance, improving user interfaces to make them more intuitive and user-friendly can significantly enhance the overall experience. Integrating AI-driven threat detection could offer more advanced security measures by identifying unusual login activities or potential threats. Expanding functionalities to include secure note and document storage can centralize sensitive information management. Offering customizable security policies would allow users to tailor password management practices to their specific needs. Embracing emerging authentication methods like biometric security and hardware keys can provide additional layers of protection. Enhanced backup and recovery options are crucial to ensure data can be restored in case of device loss or failure. Educational resources and customizable notifications can empower users to make informed decisions about their security. Lastly, providing a range of pricing plans, including cost-effective options for different user groups, can make advanced security features more accessible to a broader audience. By addressing these areas, password managers can offer a more comprehensive, secure, and user-centric experience.

4.1 Code submission (Github link)

Link: https://github.com/aryanghaoi/upskillcampus-/tree/main/blob/main/python%20project

4.2 Report submission (Github link) :

Link:

https://github.com/aryanghaoi/upskillcampus-/blob/main/blob/main/PasswordManager_Aryan_USC_UCT.pdf

5 Proposed Design/ Model

In the evolving landscape of cybersecurity, password managers are essential tools that help users manage and protect their passwords. While existing solutions offer robust functionalities like secure storage, password generation, and synchronization, there is always room for enhancement.

1.User Interface and Experience:
A modern and intuitive dashboard enhances user engagement by providing easy access to frequently used features and a clear overview of security status. Interactive onboarding helps new users understand and utilize the tool effectively, while a responsive design ensures a seamless experience across different devices.

2. Advanced Threat Detection:
AI-driven security monitoring uses machine learning to detect unusual login patterns and potential threats in real time. Integrating global threat intelligence feeds keeps the password manager updated with the latest security threats, offering proactive protection.

3. Secure Storage and Notes:
Integrated document storage allows users to keep sensitive information, like financial documents or personal notes, in a secure environment. Customizable entries provide flexibility in managing various types of confidential information, beyond just passwords.

4. Customizable Security Policies:
Allowing users to set and enforce their own security policies, such as password complexity requirements and expiration periods, ensures that their security practices align with personal or organizational standards. Admin controls offer additional oversight for organizational accounts to maintain compliance with corporate policies.

5.1 High Level Diagram (if applicable)

Figure 1: HIGH LEVEL DIAGRAM OF THE SYSTEM

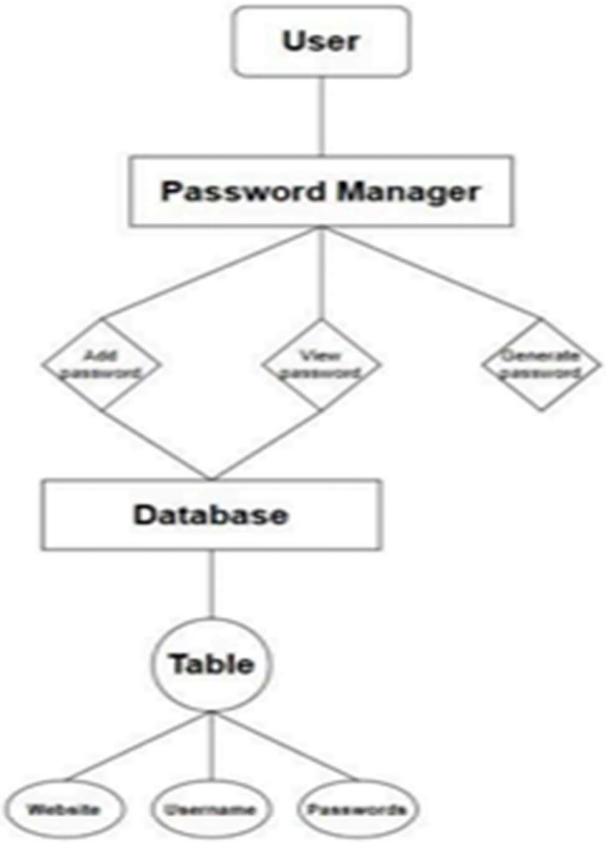


Figure 1

6 Performance Test

A focus on accuracy, power consumption, processing speed, and durability was part of the test plan to make sure the system would work well in industrial environments.

6.1 Test Plan/ Test Cases

Password Generation:

- Test Case: Verify that the password generator creates passwords meeting the specified complexity requirements (length, character types).
- Expected Result: Generated passwords should comply with the defined complexity rules**.**

Password Storage:

- Test Case: Ensure passwords are stored securely with encryption and can be retrieved correctly.
- Expected Result: Stored passwords should be encrypted, and retrieval should be accurate without exposing plaintext**.**

Auto-Fill and Auto-Login:

- Test Case: Test the auto-fill functionality in different browsers and apps.
- Expected Result: Credentials should be correctly auto-filled into the appropriate fields, and auto-login should function as intended.

Response Time:

- Test Case: Measure the response time for auto-fill, login, and data retrieval actions.
- Expected Result: Response times should be within acceptable limits for smooth user experience.

6.2 Test Procedure

The test procedure for the advanced password manager involves a systematic and thorough evaluation to ensure all functionalities, security features, and user experiences meet the defined requirements. Initially, functional testing verifies that core features such as password generation, storage, auto-fill, and secure document management operate correctly and according to specifications.

6.3 Performance Outcome

The performance outcome of an advanced password manager is assessed by measuring response times, load handling, data synchronization, resource utilization, and concurrency performance. Ideally, the system should exhibit minimal latency in key operations, efficiently manage high user loads, and ensure swift and accurate data synchronization across devices. It should utilize system resources effectively, handle concurrent operations without conflicts, and demonstrate resilience under extreme conditions during stress testing. Scalability is also crucial, with the system capable of growing to accommodate increasing users and data volumes without significant performance degradation.

7 My learnings

I learned a lot and got practical experience during this internship, which will help me advance in my profession. In order to create a workable object detection solution, I had to learn how to combine embedded systems with Internet of Things technologies. This improved my comprehension of real-time data processing and system architecture. I learned how to overcome obstacles like maximizing power usage, guaranteeing precise recognition, and efficiently handling data transfer from this experience.

In addition, by tackling and overcoming limitations in processing speed, accuracy, and durability, I strengthened my problem-solving abilities. My ability to apply theoretical knowledge in real-world circumstances has improved via working on a real-world project, which is essential for resolving challenging industrial problems.

All things considered, these knowledge and expertise will be extremely helpful as I grow in my work, especially in positions involving embedded systems, the Internet of Things, and industrial automation. They have equipped me with the skills I need to tackle technological difficulties, come up with creative solutions, and successfully participate in next initiatives and career prospects.

8 Future work scope

The future scope of an advanced password manager includes incorporating advanced AI and machine learning for improved security and personalized recommendations, integrating emerging authentication methods like biometrics and multi-factor authentication, and expanding compatibility with various devices and applications. Additionally, future developments may explore blockchain technology for decentralized security, adapt to evolving regulatory and privacy standards, enhance user education and support, and offer flexible deployment options. Embracing these advancements will help address emerging security challenges, enhance user experience, and keep pace with technological progress.