University of Sulaimani

College of Science

Computer Science

SecurePass Pro

Prepared by:

Lawand Rebwar Othman

Mohammed Abubakr Abdulla

Content

- Introduction
- Project Objectives
- System Overview
- Key Features
- User Interface Design
- Security Considerations
- Technologies Used
- Testing & Validation
- Limitations & Future Improvements
- Conclusion & References

Introduction

In the modern digital era, weak passwords remain a leading cause of security breaches. SecurePass Pro helps users generate strong passwords and analyze their security based on established best practices.

Project Objectives

1

Generate Strong Passwords

Create robust and secure passwords.

2

Analyze Strength

Evaluate password security effectively.

3

Educate Users

Promote best practices in password security.

4

Multi-Language UI

Provide a user-friendly interface in multiple languages.

5

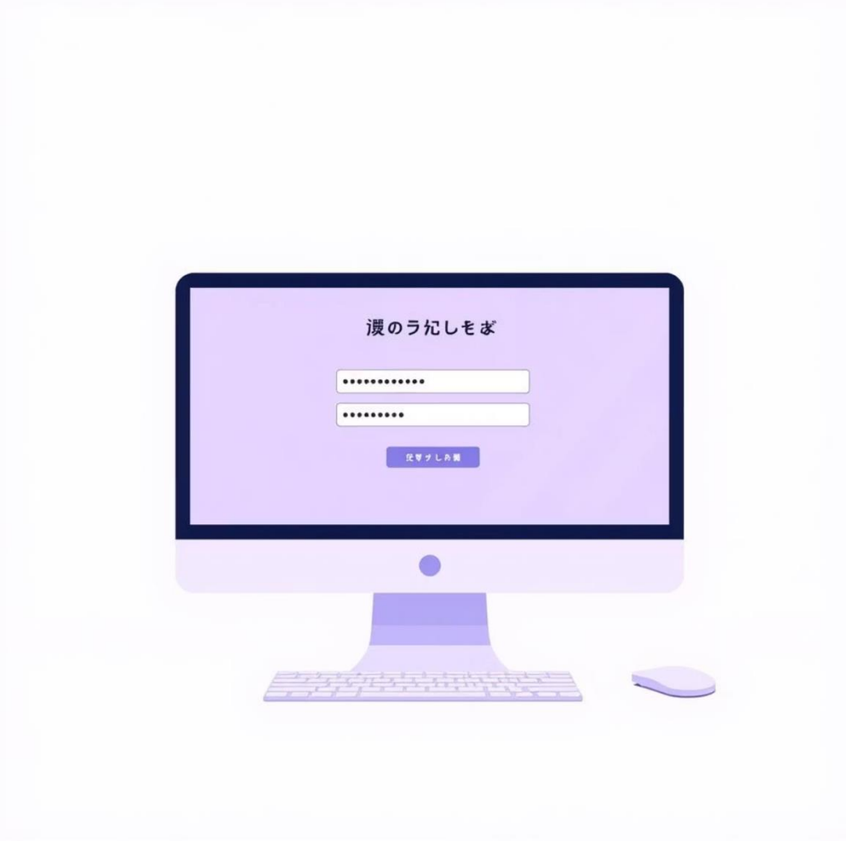
Simplicity & Usability

Ensure an intuitive and easy-to-use experience.

System Overview

SecurePass Pro is a standalone desktop application designed to help users create and evaluate secure passwords. Crucially, it operates without storing any sensitive data, prioritizing user privacy and data security.

Its offline functionality ensures that generated passwords and analyses remain entirely on the user's device, mitigating risks associated with cloud storage.



Key Features

Password Generation

Utilizes letters, numbers, and symbols for robust password creation.

Strength Checking

Evaluates password strength against security standards.

Show/Hide Password

Toggle visibility for convenience and security.

Copy to Clipboard

Easily transfer generated passwords.

Clear Input Fields

Quickly reset and clear all input data.

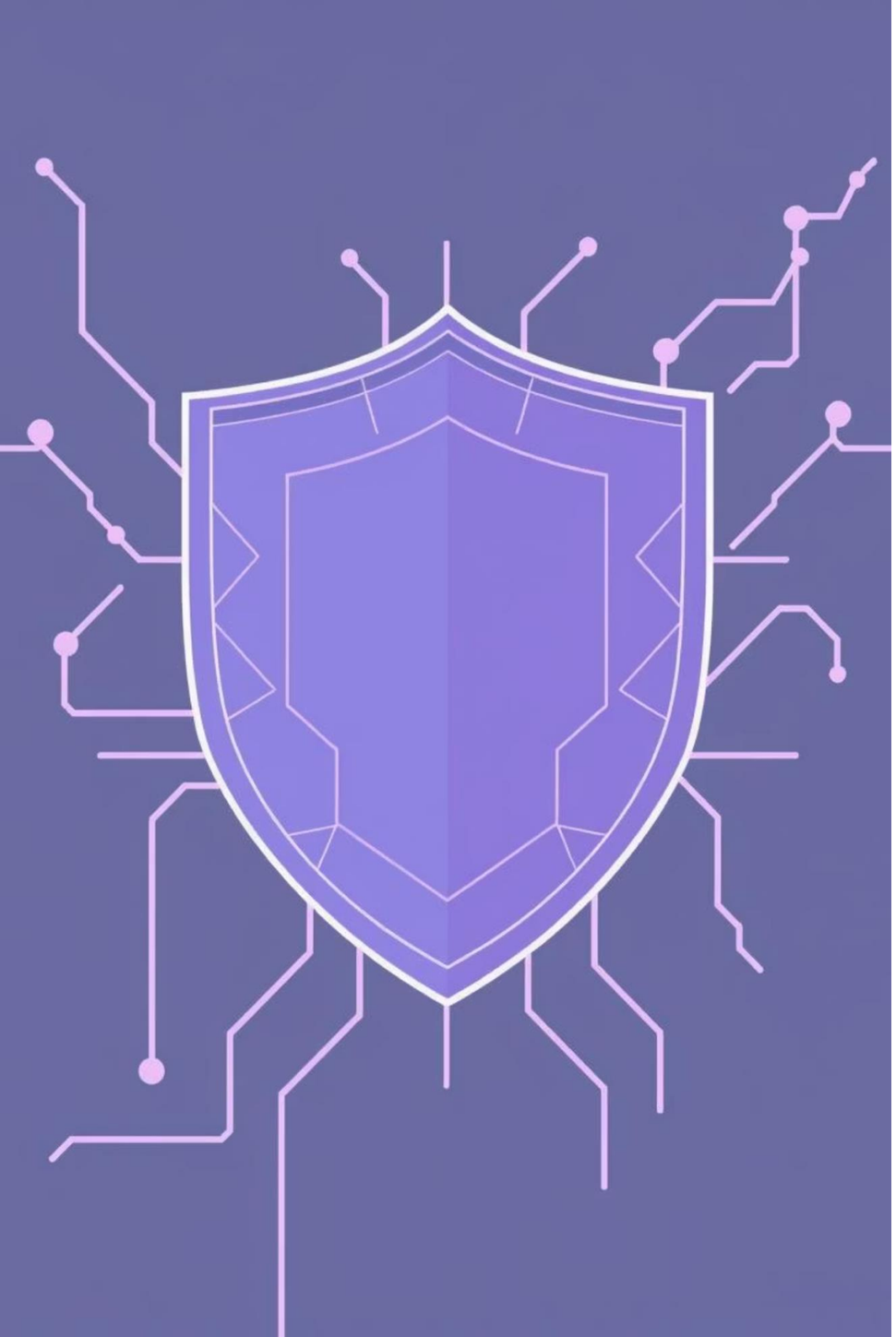
Multi-Language Support

Accessible to a diverse global user base.

User Interface Design

The application features a dark-themed professional interface, meticulously designed to minimize eye strain and enhance overall usability. This aesthetic choice contributes to a comfortable user experience, especially during prolonged use.

Buttons and input fields are intuitively organized, ensuring clear navigation and straightforward interaction. The layout prioritizes user efficiency, making password management simple and effective.



Security Considerations

No Password Storage

Passwords are never stored permanently, ensuring maximum privacy.

Offline Operation

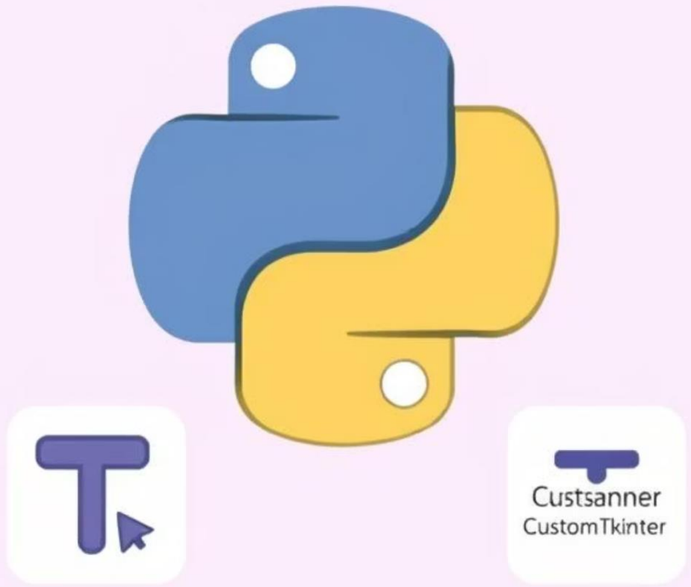
The application runs entirely offline, eliminating online vulnerabilities.

Random Generation

Utilizes robust random methods for secure password creation.

User Privacy

Designed with user privacy and data security as top priorities.



Technologies Used

Python Programming Language

The core language for application logic and functionality.

Tkinter / CustomTkinter

Used for building the graphical user interface (GUI).

Python Standard Libraries

Leveraged for various essential functionalities.

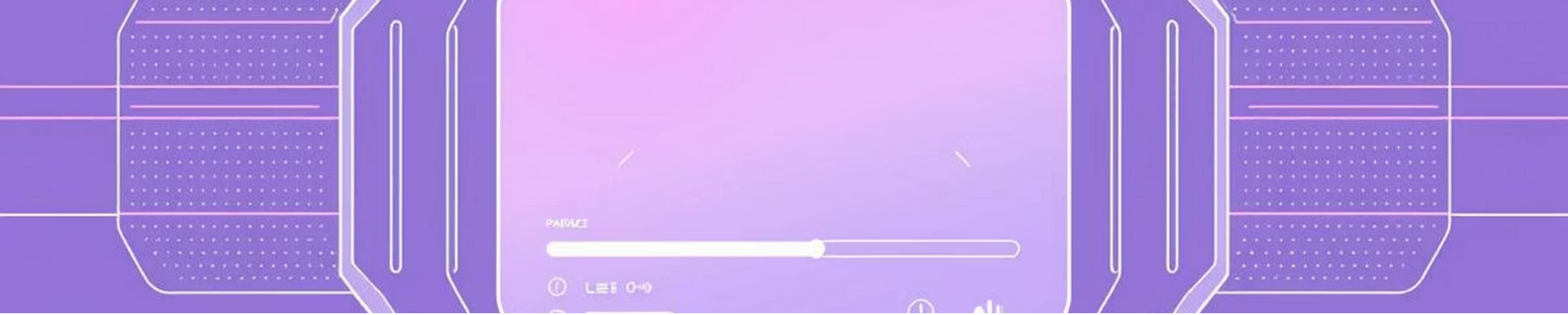
Custom Translation Module

Enables multi-language support within the application.

Testing & Validation

SecurePass Pro underwent rigorous testing to ensure its reliability and effectiveness. The application was thoroughly evaluated using a range of password types: weak, medium, and strong.

This comprehensive testing verified the accuracy of its strength classification algorithms and confirmed stable performance across all scenarios, guaranteeing a dependable user experience.



Limitations & Future Improvements

Current Limitations

- No cloud password storage
- No password history saving
- Clipboard does not auto-clear

Future Enhancements

- Password length customization
- Character selection options
- Strength progress bar
- Password entropy score
- Clipboard auto-clear feature

Conclusion & References

SecurePass Pro is a professional desktop application showcasing strong programming skills, security awareness, and user-focused design. It successfully promotes better password practices.

NIST Password Guidelines

OWASP Authentication Best Practices

Python Official Documentation