C3F1

RESEARCH AND PROJECT PRESENTATION

PROPOSED BY TEAM 3:
CALÒ DOMENICO, CAPUANO MARZIA, CRISPINO LUCA, FICARELLA FABRIZIO

16 Jan, 2025

OVERVIEW

BACKGROUND OF THE STUDY

This research outlines the development process and design considerations of a secure and user-friendly Password Manager, called C3F1. The project was conceived to address the increasing need for robust cybersecurity solutions in an era where digital threats continue to grow with great frequency and sophistication. Our team collaborated to design a solution that adresses critical need for robust cybersecurity in today's digital landscape

C3F1

PROBLEM STATEMENT

Our study focuses on evaluating the market landscape, consumer trends, and competition pertinent to the new product.

01

SCOPE OF THE STUDY

This report outlines the development process and design considerations of a secure and user-friendly Password Manager called C3F1.

02

RELEVANCE OF THE STUDY

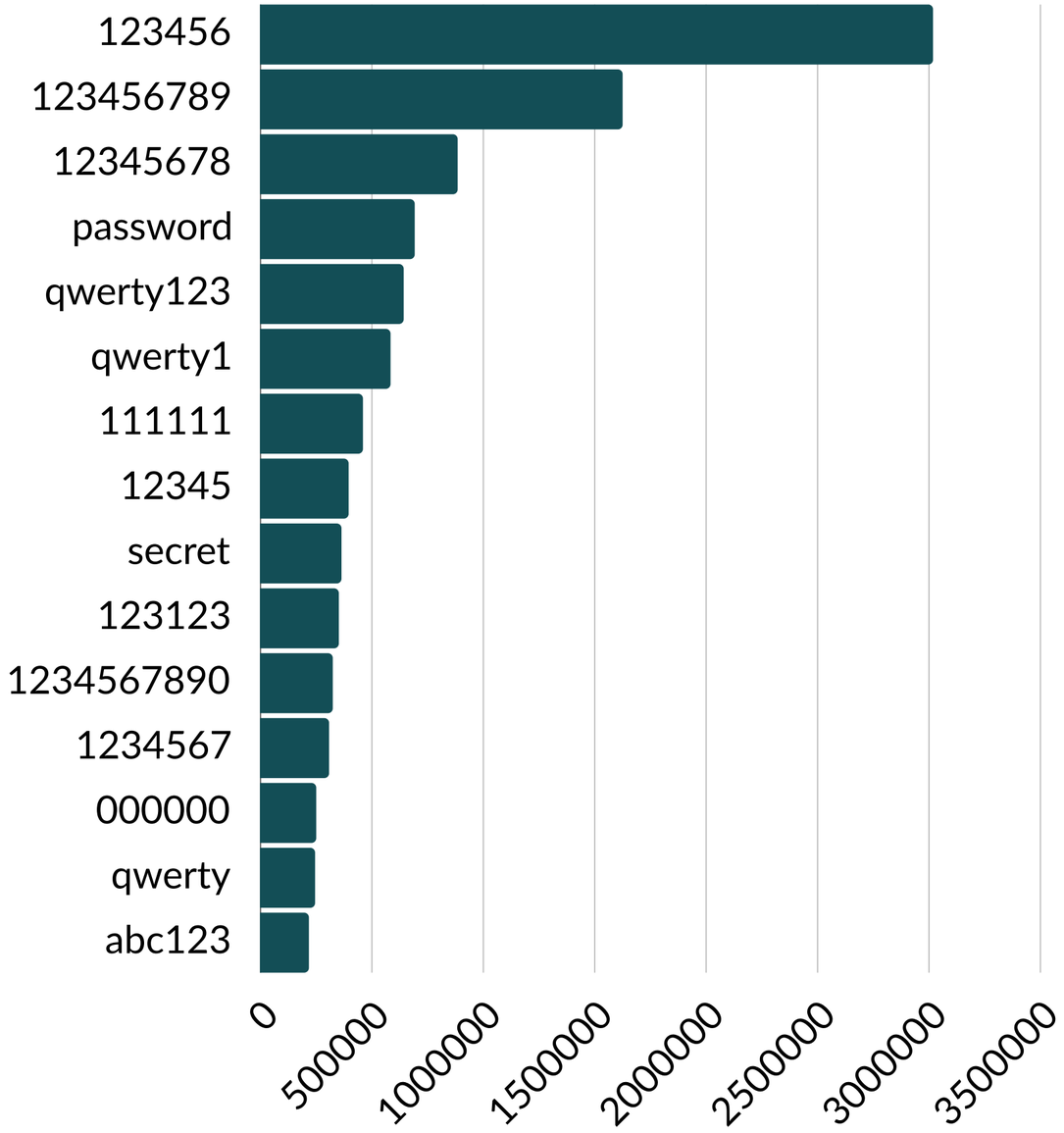
This PM emphasizes best practices in cybersecurity by promoting the adoption of strong passwords for all accounts. By solving the risks with weak or reused passwords, the project reduce the likelihood of data breaches and improves overall security hygiene.

03

PM‘S ANALYSIS

To establish a robust foundation for developing our password manager, we conducted an in-depth analysis of several existing solutions that are widely utilized by the community

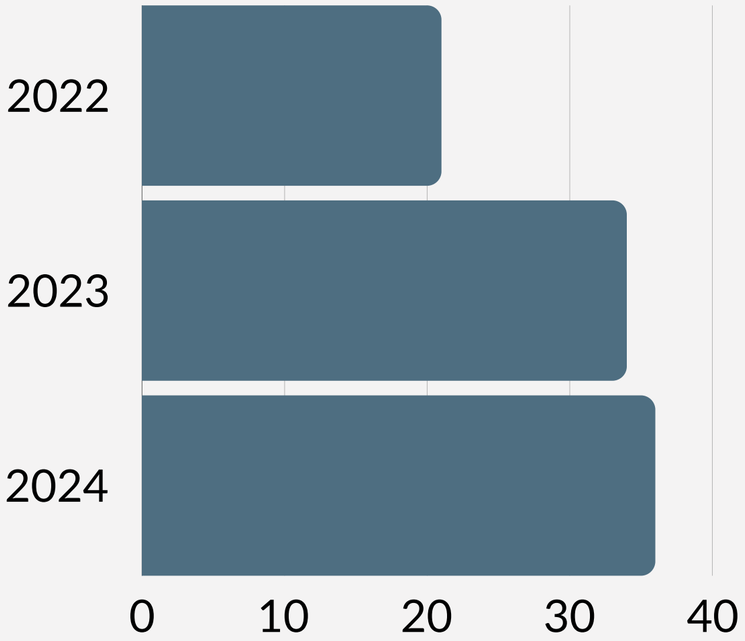
REPORT'S RESULTS ANALYSIS



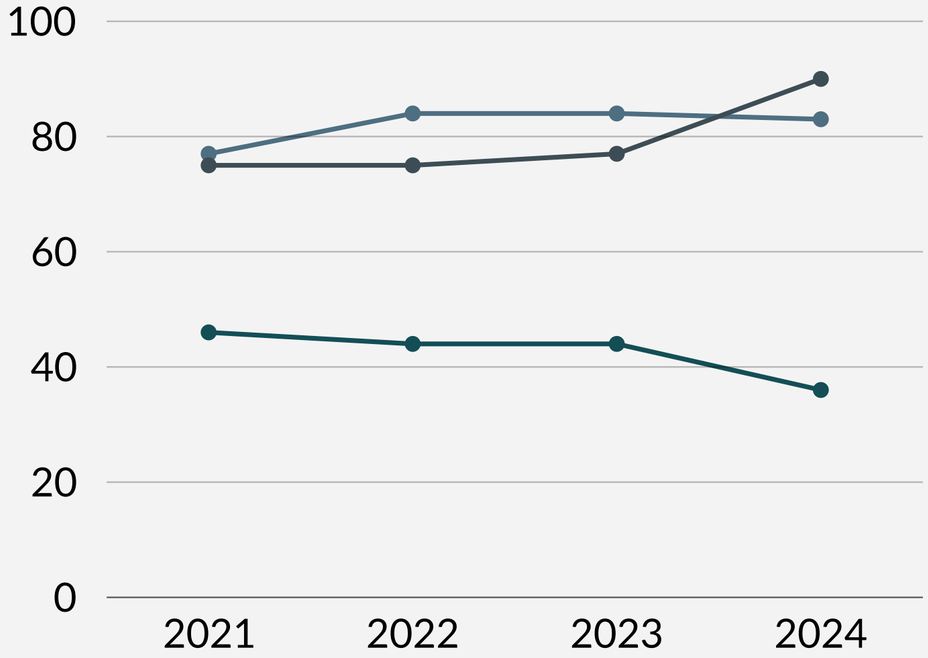
MOST COMMONLY USED PASSWORD

Many users continue to rely weak and easily guessable password. This behavior stems for cognitive limitations in generating and remembering unique and complex password for each account

TRENDS ANALYSIS



Adoption trends of password manager in the US



Trend on devices on which password manager are installed

PM	Free Version	Biometric Access	Key Features
pCloud Pass	Yes	Yes	Lifetime subscription, customizable password generator, lacks tag-based organization
NordPass	Yes	Yes	Zero-knowledge encryption, breach monitoring, 2FA support
Dashlane	Yes	Yes	Dark web monitoring, autofill, 2FA support, corporate credential management
1Password	No	Yes	Passwordless access, encrypted document storage (1 GB), credential recovery
Kaspersky PM	14-day trial	Yes	Secure password generator, encrypted cloud storage, synchronization across devices
Keeper	30-day trial	Yes	Dark web monitoring, encrypted messaging, secure password sharing
RoboForm	Yes	Yes	Offline access, AES-256 encryption, TOTP-based 2FA, folder-based organization

COMPARISON OF PASSWORD MANAGERS

Comparison of the Password Managers which we have consider in our state-of-art analysis inside our report.

SPRINTS' OVERVIEW

1

DOCUMENTATION AND FINAL EXPLORATION

We focused on gathering the necessary background information and documentation to ensure that our project was well-founded and could be implemented effectively.

2

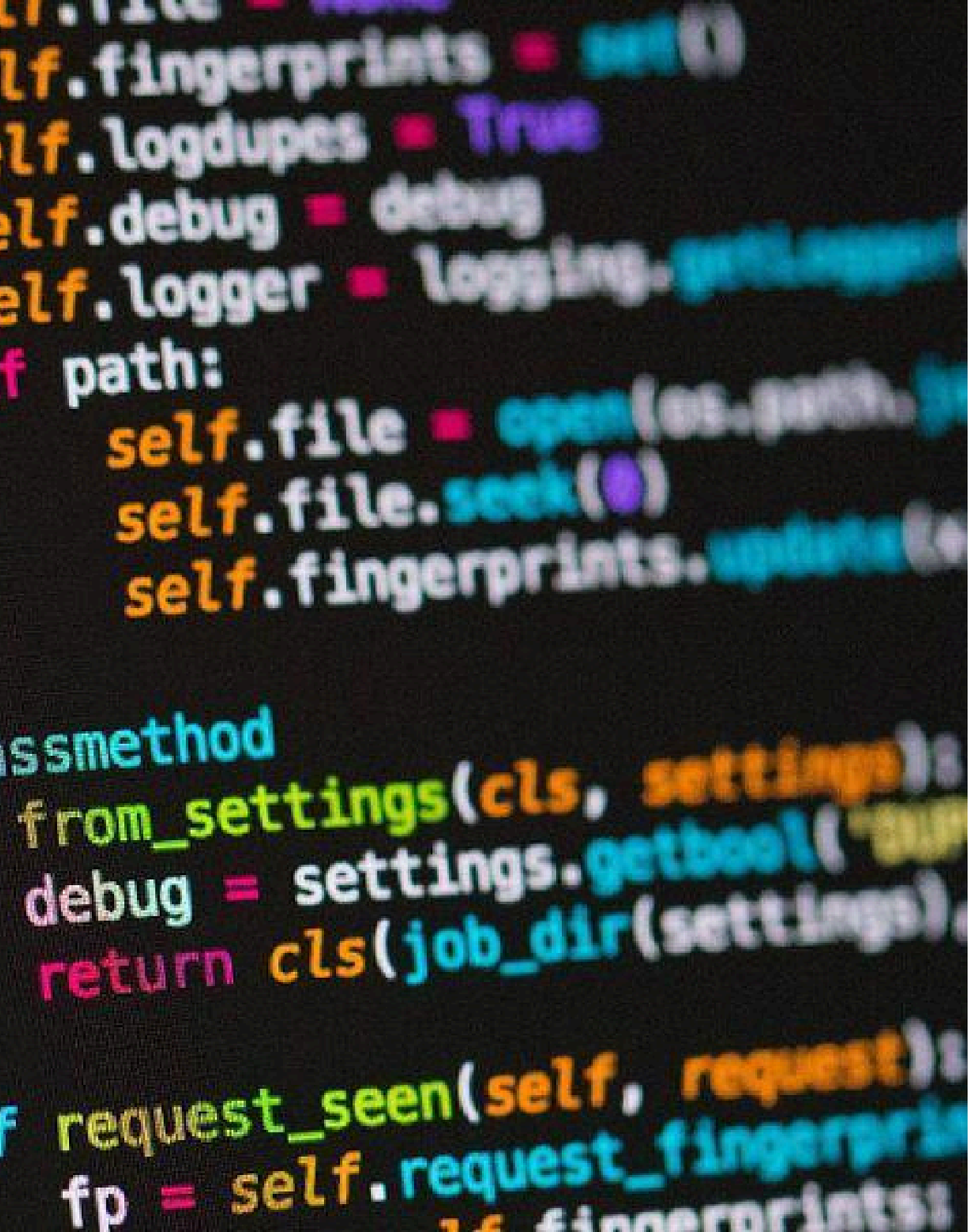
IMPLEMENTATION AND VERSIO CONTROL

We focused on implementing the core part of the project. In addition to this, we also implemented a versioning strategy to help manage the updates and changes made to the project throughout the sprint.

3

FINAL REVIEW AND REPORT WRITING

This final sprint was focused on finalizing the project code and preparing the final report.



DESIGN DECISIONS

Our password manager will use React and Flask, respectively, for the frontend and backend. Moreover, it uses Google Authenticator to produce valid TOTPs

Flask

FUNCTIONAL REQUIREMENT:

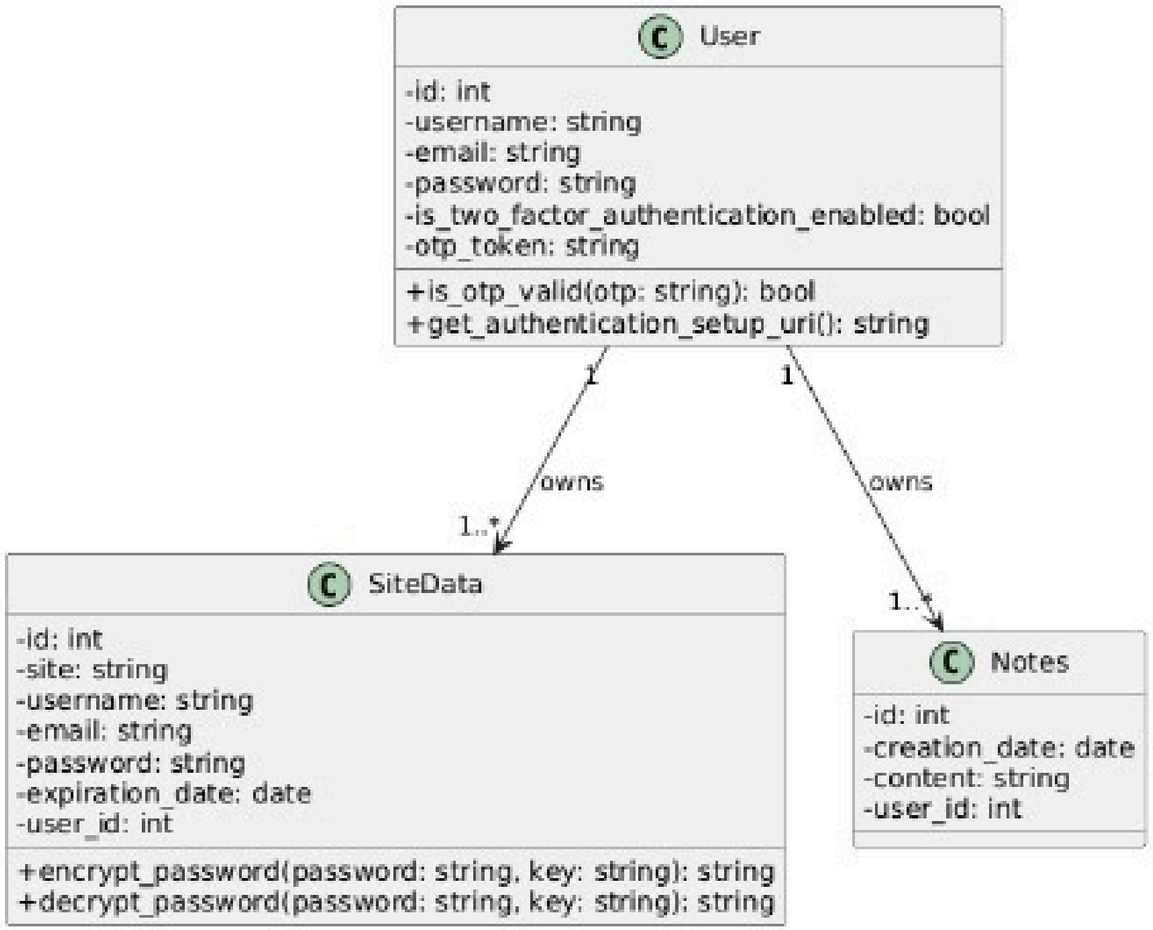
- Random password generator
- TOTP verification
- Secure storage
- Cross-platform usage

NON-FUNCTIONAL REQUIREMENT:

- Security
- Reliability
- Portability
- Usability

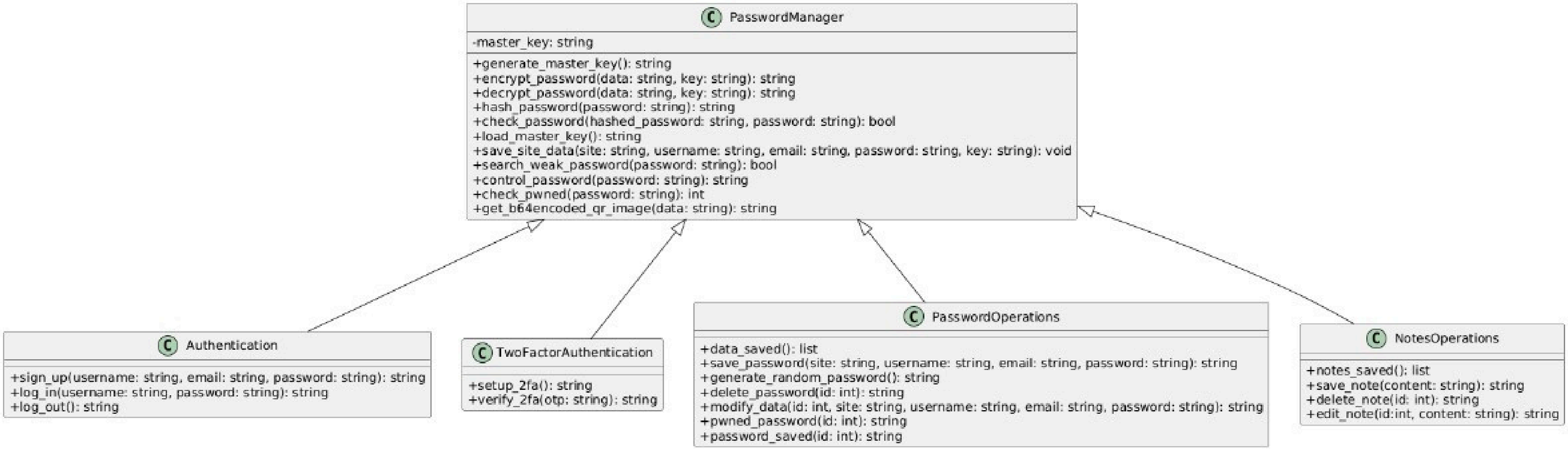
APPLICATION STACK

Models



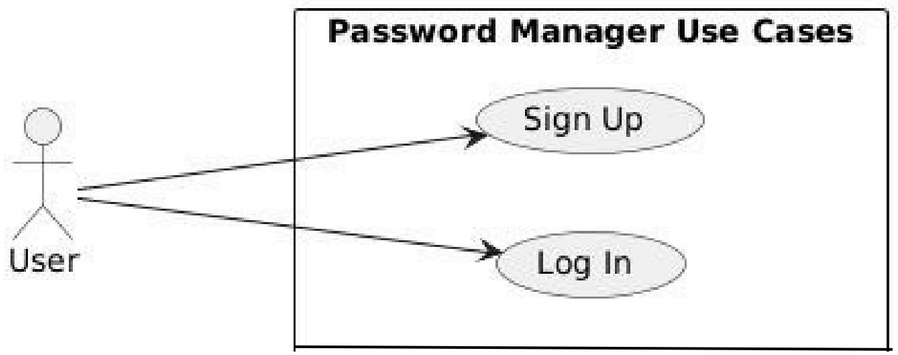
APPLICATION STACK

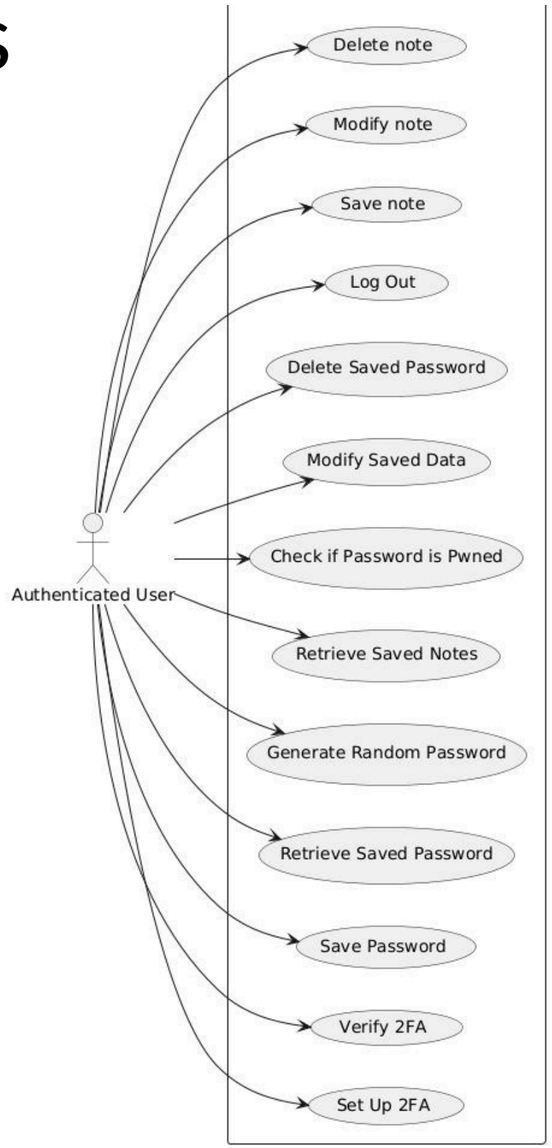
Function



APPLICATION STACK

Interactions





CONCLUSION AND FUTURE WORK

- SSL/TLS
- Password Sharing
- Autofill
- Deployment of the Application
- Other methods of 2FA
- Loading animation

C3F1

THANK YOU

16 Jan, 2025