CS301.1 Investigative Studio

Written by Conor Cook

Working with Nicki Choo

Supervisor, Rouwa Yalda

Contents

[Abstract: 2](#_Toc161320919)

[Introduction: 2](#_Toc161320920)

[Literature Review 3](#_Toc161320921)

[Article 1: A Study for an Ideal Password Management System 3](#_Toc161320922)

[Article 2: Balancing Password Security and User Convenience: Exploring the Potential of Prompt Models for Password Generation 3](#_Toc161320923)

[Article 3: A comparative study on Modern Password Management 4](#_Toc161320924)

[Article 4: A Dynamic Method and Program for Multiple Password Generation and Management 4](#_Toc161320925)

[Article 5: Revisiting Security Vulnerabilities in Commercial Password Managers 4](#_Toc161320926)

[Summary: 5](#_Toc161320927)

[Research Question: 6](#_Toc161320928)

[Changes to be Made: 6](#_Toc161320929)

[New Features: 6](#_Toc161320930)

[Improvements: 7](#_Toc161320931)

[Schedule for Implementation/Timeline: 8](#_Toc161320932)

[Tools: 8](#_Toc161320933)

[GitHub: 8](#_Toc161320934)

[Trello: 8](#_Toc161320935)

[Conclusion: 9](#_Toc161320936)

[References 10](#_Toc161320937)

[Notes (For personal use) 10](#_Toc161320938)

# Abstract:

In the modern age of the internet, passwords have become an essential. With how often a password is needed online, it gets challenging to remember all of them. Therefore, people have developed a product called a password manager. A password manager stores a user’s login details and keeps them secure. Several hundred password managers exist online, some even built into a browser, but the issue related to these tools are related to either being secure but not user friendly, or not secure but very user friendly. In 2023 a password manager, called MasterVault, has been deployed with the aim to balance user-friendly design with enhanced security. It had an excellent design, but it fell short of the original intentions and was not able to deliver all it had promised to do. This project aims to enhance MasterVault, making it an ideal password manager that perfectly balances security with user-friendly design.

# Introduction:

Password managers need to be secure, as they store incredibly important user information. However, a lot of easily accessed password managers have next to no security. Browser-based password managers are an excellent example. There have been several studies stating that browser-based password managers are not secure and have been a part of several private data leaks. But they are by far the easiest password managers for users as they are built into the browser. Meanwhile a well know password manager called ‘Dashlane’ (*Dashlane password manager* 2024), which is widely considered one of the best password managers on the market, is not very user-friendly. This imbalance causes users who are not experienced with password managers to primarily use browser-based password managers, which as stated before, are not secure. This leaves a large number of users online vulnerable to their private information being stolen. MasterVault aimed to fill this gap in the password manager market. By implementing several security features like 256-AES encryption, master passwords and account locking all while having a user-friendly interface. However, when the product was released, it wasn’t able to deliver all it promised to be.

The aim of this CS301.2 project it to enhance MasterVault. Adding new features to make it more secure and user-friendly. But also improving what was already developed. By the end of this project, MasterVault will be the ideal password manager for users of all backgrounds and experiences.

# Literature Review

## Article 1: A Study for an Ideal Password Management System

*(Shinde & Deshpande, 2022)*

This article discussed the requirements for a password manager to be secure and usable. Users usually opt for weaker passwords due to the cognitive load of recalling complex passwords. In terms of password generation, password managers that are designed for simplicity typically have a limited symbol set used in generation. The authors found that KeePass has one of the most comprehensive symbol sets. The article states that a secure password manager should use 256-AES encryption, however there are various methods used for meta data encryption among password managers. The authors then discussed the importance of user engagement to prevent unauthorised access through functions like autofill. In addition, valuable insights for creating an ideal password manager that emphasises the significance of password strength and encryption standards.

## Article 2: Balancing Password Security and User Convenience: Exploring the Potential of Prompt Models for Password Generation

*(Umejiaku et al., 2023)*

This article highlights the important of strong passwords in the face of cyber-attacks and data breaches. Modern password generation can create incredibly secure and complex passwords, it often results in password that are far too hard to remember, causing users to reuse or write the password down. However, prompt models such as ChatGPT are presented as solutions to generate strong and memorable password generators, tailored to the users.

The author of this article used Pass fault to evaluate the strength of passwords generated by ChatGPT, while applying rules to modify the passwords. Some of the rules used in the study include changing vowels with characters, replace the most common vowel, remove all vowels and more. The results indicate that the modify passwords had improved strength, particularly when the vowels of a password were changed. While passwords generated by prompt models posed security concerns. The article concludes by emphasizing the need for reasonable password standards and considering prompt models as tools to balance security and user convenience.

## Article 3: A comparative study on Modern Password Management

*(Aman Pratap Singh, 2021)*

This article discusses the importance of password managers in the digital age, highlighting the increasing threats from attackers and hackers. The articles emphasise the need for a secure password manager. The article suggests that most password managers are considered safe, there are various risks when storing sensitive information. The research suggests the idea of using passphrases as a secure alternative to regular passwords. The author states that passphrases are easier to understand, remember and harder to hack. The article explores strengthening passwords through paraphrases and discusses their application in protecting SSH and private keys used in email encryption tools.

## Article 4: A Dynamic Method and Program for Multiple Password Generation and Management

(Citation needed)

This article discusses the challenges associated with the increasing number of passwords users need for various online services and the potential security risks involved. It introduces different approaches to password management, such as password managers, password generators, and specific methods like Site-Specific Passwords and Password Multiplier. The article then delves into the Chinese Remainder Theorem and proposes a dynamic method and program for multiple password generation and management based on the Forward Direction Method. This method involves determining a strong unique password and generating divisors to obtain individual passwords. The article highlights the security advantages of this approach, where only divisors are stored, making it difficult to retrieve the unique password even with knowledge of the divisors. The results and discussion section provides sample individual passwords generated using this method and emphasizes the numerical size difference between the unique password and divisors, enhancing security.

## Article 5: Revisiting Security Vulnerabilities in Commercial Password Managers

(Citation needed)

This article explores recently found problems as well as vulnerabilities that have been made in popular password managers. The vulnerabilities that have been found include two-factor authentication seed, element inspection, registration discovery, HTTP(S) autofill and ignoring subdomains. The study reveals that most password managers are susceptible to, HTTP(S) autofill, and ignoring subdomains vulnerabilities. Additionally, the article highlights new vulnerabilities, such as brute force attacks, a phishing attack, a clipboard vulnerability, and a PIN brute force vulnerability. The authors emphasize responsible disclosure efforts, describing their interactions with vendors and how they addressed the vulnerabilities that were identified. They also acknowledge the advantages and disadvantages of company’s reactions to the concerns that were exposed. To improve overall security, the article suggests creating strict security models and canonical security tests for password managers.

## Summary:

All five of these articles have talked about various elements of security with password managers and how to improve password security. Using these articles, they will help us to improve MasterVault to an ideal password manager for anyone to use.

# Research Question:

After reviewing the previous articles, we came up with the following research question:

“How can password managers evolve and adapt to security threats and user preferences while maintaining user-friendliness?”

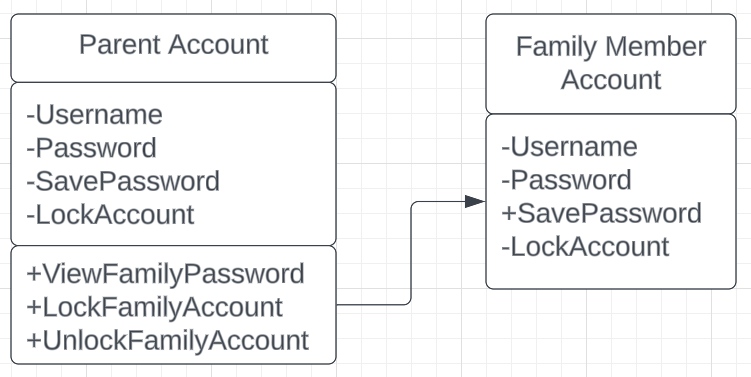
# Changes to be Made:

## New Features:

* Saving different login details

Currently with MasterVault, you can only save three details at one. Those details being website, email/username, and password. However, some websites require more details for login. We aim to add new login details that users can save when saving a password with the password manager. These new login details will be Date, Number and Other. Other will be a text input which can be used for anything that does not fit into the other fields.

* Adding types of account options

Modern password managers only have one account option, a personal account. No one has explored the potential of group account types, like family accounts. We intend to explore this new potential by adding option account types. Below is a UML diagram, explaining how we intend a family account will work.

* Search & Filter

MasterVault has the ability to store a very large amount of passwords. But it may prove difficult to find the password you want. Giving the user the ability to search for and filter their passwords will greatly improve the user experience.

* Secure/lock passwords

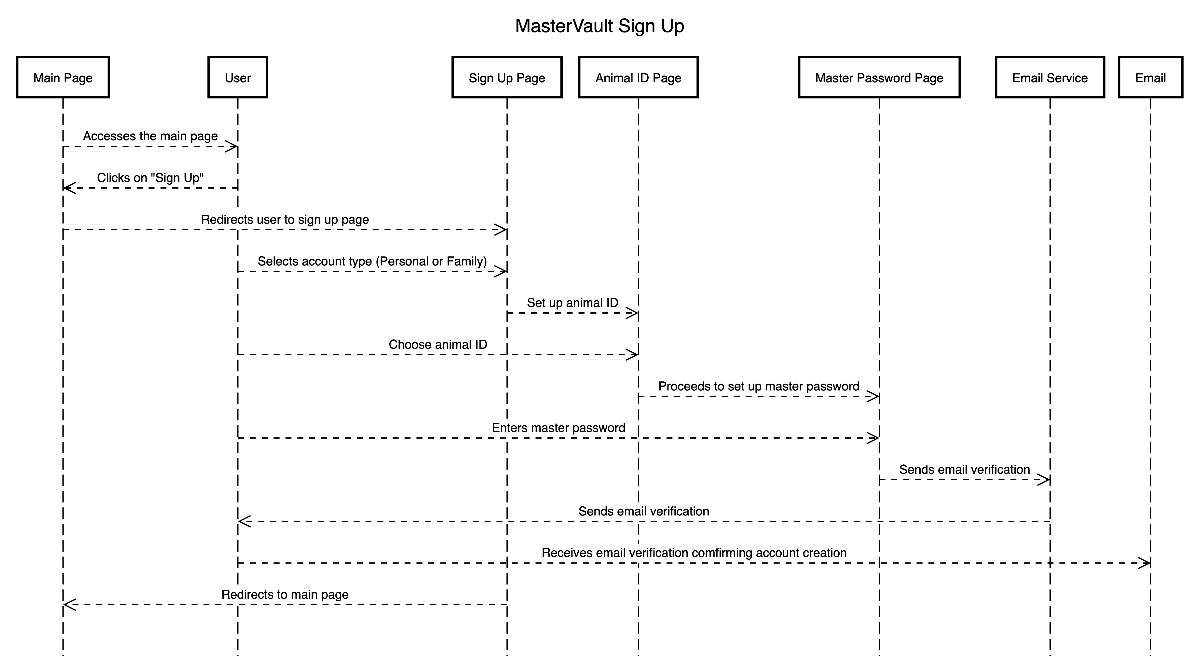
With regular password managers, all the users’ passwords are visible on the same page. However, some passwords might be far more important than others. Giving user’s the ability to lock their password, only to be unlocked with a master password, will help users feel that their passwords are very secure.

## Improvements:

* 256-AES Encryption

As stated, before in the literature review above. 256-AES encryption is considered the industry standard for password managers. Implementing 256-AES encryption will add a lot of security to the password manager.

* Securer login

When investigating MasterVault, it felt like the account login was not very secure. Taking inspiration from Malaysian online banking, when a user logs into their account they are prompted with a photo of an animal they’ve selected prior. The user must then confirm whether the animal being presented is the one they selected prior. Below is a sequence diagram showing how this feature will work when the user creates a MasterVault account.

* Move MasterVault to online

MasterVault is currently bound to being a local system use product. Moving the product online will make it easier for users to use MasterVault.

* Paraphrase Generator

One of the articles reviewed for this proposal explored the potential for using paraphrases to enhance passwords. MasterVault already has a keyword based password generator, we plan on enhancing this generator to paraphrase passwords for users.

# Schedule for Implementation/Timeline:image

# Tools:

There will be two main tools used for the development of this project.

## GitHub:

(Wanstrath et al., 2008)

GitHub will be used for code collaboration. It has been a stable product for collaboration, and we have plenty of experience using it in the past.

## Trello:

(Cannon-Brookes & Farquhar, 2011)

Trello is a project management tool. It allows us to have a visual representation of tasks using lists and cards. It allows us to assign work to teammates and track the progress of one another and the progress of the project.

# Conclusion:

In conclusion, modern day password managers all have area in which they excel. But they all fall short in one area or another, leaving a large amount of users unable or unwilling to use the password manager. MasterVault aimed to fill this gap in the market but fell short. We aim to enhance MasterVault by adding top-of-the-line security and make it as user-friendly as possible. By the end of this project, we believe MasterVault will be an ideal password manager for all users online.

# References

* *Dashlane password manager*. Dashlane. (2024, March 7).

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

* Shinde, S., & Deshpande, M. (2022). *IJRASET Journal for Research in Applied Science and Engineering Technology*. A Study for an Ideal Password Management System. <https://www.ijraset.com/research-paper/an-ideal-password-management-system>
* Umejiaku, A. P., Dhakal, P., & Sheng, V. S. (2023, May 9). *Balancing password security and user convenience: Exploring the potential of prompt models for password generation*. MDPI. <https://www.mdpi.com/2079-9292/12/10/2159>
* Aman Pratap Singh, G. S. (2021). *A comparative study on modern password management*. <https://annalsofrscb.ro/index.php/journal/article/view/9761>
* (Article 4)
* (Article 5)
* Wanstrath, C., Preston-Werner, T., & Hyett, P. J. (2008). *Let’s build from here*. GitHub. <https://github.com/>
* Cannon-Brookes, M., & Farquhar, S. (2011). *Trello brings all your tasks, teammates, and tools together*. Trello. <https://trello.com/>

# Notes (For personal use)

* Articles
  + [A Dynamic Method and Program for Multiple Password Generation and Management](https://dergipark.org.tr/en/pub/ject/issue/64442/1031900)