

# Usable Study Report

By Vasanth and Devi Sri Charan

## Proposal for SecurePass

SecurePass is a web extension that provides an additional layer of security for users who store their passwords on their web browsers. With SecurePass, users must authenticate themselves whenever they want to access their saved passwords, ensuring that only authorized users can access their accounts.

---

## Literature Review on using 2FA for Saved Passwords

Two-factor authentication is becoming increasingly popular as a means of securing online accounts. One area where two-factor authentication can be particularly useful is in the management of saved passwords, where sensitive information is stored locally on a user's device. This literature review will explore the benefits of two-factor authentication in the context of saved passwords.

### ***Benefits of Two-Factor Authentication for Saved Passwords:***

One of the main benefits of two-factor authentication for saved passwords is adding an extra layer of security to the process. This is particularly important when sensitive information is stored locally on a device. Two-factor authentication can prevent unauthorized access to a user's passwords, even if someone has access to their device. According to research, two-factor authentication is more secure than single-factor authentication methods and can significantly reduce the risk of password-related attacks (Yu et al., 2016).

In addition to increased security, two-factor authentication can also improve user experience. By making the process of accessing saved passwords more secure and convenient, users are more likely to engage in secure password practices. This, in turn, can help to reduce the risk of password-related security breaches (**Nash, 2018**).

### ***Implementation of Two-Factor Authentication for Saved Passwords:***

There are several ways to implement two-factor authentication for saved passwords. One approach is to use a separate two-factor authentication application or device, such as Google Authenticator or YubiKey. Another approach is to use biometric authentication, such as fingerprint or facial recognition technology. Finally, some password management applications offer two-factor authentication options.

While there are various approaches to implementing two-factor authentication for saved passwords, research has shown that the most effective approach is to use a separate application or device for authentication (**Dell'Amico et al., 2017**). This approach provides an additional layer of security by separating the authentication process from the password storage process.

Two-factor authentication is a valuable tool for securing saved passwords, providing users with an extra layer of security and convenience. Using a separate application or device is the most effective approach to implementing two-factor authentication. Using two-factor authentication, users can reduce the risk of password-related security breaches and protect their sensitive information.

### **References:**

1. Dell'Amico, M., Michiardi, P., & Roudier, Y. (2017). A Survey of Two-Factor Authentication Methods in Online Services. *ACM Computing Surveys*, 49(4), 1-37.
2. Nash, C. (2018). A User-Centered Evaluation of a Two-Factor Authentication Scheme for Password Management. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1-13.

3. Yu, Z., Wang, J., Yang, Y., Wu, J., Zhang, W., & Ma, X. (2016). Enhancing Security of Password-Protected Web Services Using Two-Factor Authentication. *International Journal of Distributed Sensor Networks*, 12(2), 1-11.
- 

## Competitive Analysis

We did a competitive analysis of web extensions similar to SecurePass, the proposed two-factor authentication extension for saved passwords:

1. **LastPass:** LastPass is a popular password manager and web extension that offers two-factor authentication for added security. It also allows users to store and manage passwords, credit cards, and other sensitive information in a secure vault. LastPass offers a variety of two-factor authentication options, including Google Authenticator, YubiKey, and fingerprint authentication on mobile devices.
2. **1Password:** 1Password is a password manager and two-factor authentication solution that offers a web extension for Chrome, Firefox, and Safari. 1Password allows users to store and manage their passwords, credit cards, and other sensitive information in a secure vault. It also offers two-factor authentication via Google Authenticator or other third-party authenticator applications.
3. **Keeper:** Keeper is a password manager and two-factor authentication solution that offers a web extension for Chrome, Firefox, and Safari. Keeper allows users to store and manage passwords, credit cards, and other sensitive information in a secure vault. It offers a variety of two-factor authentication options, including SMS, fingerprint, and facial recognition on mobile devices.
4. **Dashlane:** Dashlane is a popular password manager and two-factor authentication solution that offers a web extension for Chrome, Firefox, and Safari. Dashlane allows users to store and manage their passwords, credit cards, and sensitive information in a secure vault. It offers two-factor authentication via Google Authenticator or other third-party authenticator applications.

### **Comparison:**

All web extensions offer users two-factor authentication and password management solutions. However, there are some differences between the extensions regarding features and pricing. For example, LastPass offers a free version of their extensions, while 1Password and Keeper require a subscription to use their extensions. Dashlane offers both a free and premium version of its extension.

Regarding two-factor authentication options, LastPass and Keeper offer the widest variety of authentication methods, including biometric authentication on mobile devices. Dashlane offers a more limited range of options, while 1Password only offers Google Authenticator.

Overall, each of these web extensions has its unique features and benefits. Users should evaluate each option based on their individual needs and preferences. SecurePass, the proposed extension, would need to offer comparable features and functionality to compete with these established players in the market.

---

### **Survey Questions ([Link](#))**

We conducted surveys to develop a broad understanding of our problem space.

Below are questions that we made for the survey

1. What is your current password management process like?
  - I use a password manager app
  - I save passwords in my browser
  - I write passwords down on paper
  - Other (please specify): \_\_\_\_\_
2. Have you ever had any security issues with your saved passwords?
  - Yes
  - No

- Not sure
3. Have you ever used a password manager or two-factor authentication solution before? If so, which one(s)?
    - LastPass
    - 1Password
    - Google Authenticator
    - Authy
    - YubiKey
    - Other (please specify): \_\_\_\_\_
    - I have not used any password manager or two-factor authentication solution
  4. What are some of the main challenges you face with password management and two-factor authentication?
    - Keeping track of passwords
    - Remembering which password goes with which account
    - Two-factor authentication takes too much time
    - Two-factor authentication is inconvenient
    - Security concerns
    - Other (please specify): \_\_\_\_\_
  5. How do you balance convenience with security when it comes to password management?
    - I prioritize convenience over security
    - I prioritize security over convenience
    - I try to find a balance between convenience and security
  6. How important is it to you to have access to your saved passwords across all your devices?
    - Very important
    - Somewhat important
    - Not very important
    - Not important at all
  7. How familiar are you with two-factor authentication?
    - Very familiar
    - Somewhat familiar

- Not very familiar
  - Not familiar at all
8. Have you ever used two-factor authentication before? If so, which method(s) did you use?
- SMS code
  - Authenticator app
  - Hardware token (e.g., YubiKey)
  - Other (please specify): \_\_\_\_\_
  - I have not used two-factor authentication
9. What do you perceive as the benefits of using two-factor authentication?
- Extra security
  - Protection against hacking and identity theft
  - Peace of mind
  - Other (please specify): \_\_\_\_\_
10. What do you perceive as the challenges of using two-factor authentication?
- Takes too much time
  - Inconvenient
  - Difficulty setting up
  - Other (please specify): \_\_\_\_\_
11. How do you feel about the idea of a web extension that provides two-factor authentication for saved passwords?
- Very interested
  - Somewhat interested
  - Not very interested
  - Not interested at all
12. What features do you look for in a password manager or two-factor authentication solution?
- Easy-to-use interface
  - Cloud backup and synchronization
  - Ability to generate strong passwords
  - Multiple two-factor authentication options
  - Support for multiple devices
  - Other (please specify): \_\_\_\_\_

---

## Interview Questions ([Link](#))

We also conducted interview to develop a broad understanding of our problem space. Below are questions that we asked the interviewee (section-wise).

### **Section 1: Password Management**

1. What is your current password management process like?
2. Have you ever had any security issues with your saved passwords?
3. Have you ever used a password manager or two-factor authentication solution before? If so, which one(s)?
4. What are some of the main challenges you face with password management and two-factor authentication?
5. How do you balance convenience with security when it comes to password management?
6. How important is it to you to have access to your saved passwords across all your devices?

### **Section 2: Two-Factor Authentication**

7. How familiar are you with two-factor authentication?
8. Have you ever used two-factor authentication before? If so, which method(s) did you use?
9. What do you perceive as the benefits of using two-factor authentication?
10. What do you perceive as the challenges of using two-factor authentication?
11. What additional security features would you like to see in a two-factor authentication solution?

### **Section 3: SecurePass Web Extension**

12. How do you feel about the idea of a web extension that provides two-factor authentication for saved passwords?
  13. What features do you look for in a password manager or two-factor authentication solution?
  14. How would you describe your technical skills and comfort level with using new technology?
-

## Low-Fidelity Prototype ([Link](#))

Create new account

Username

Email

Already have an account, login?

Username

\*\*\*\*\*

Use Saved Password

Create new account


Username

Email

Already have an account, login?

If you want to use the saved password

Scan your Fingerprint



Create new account

Username

Email

Already have an account, login?

If you want to use the saved password

Enter the PIN

123

Create new account

Username

Email

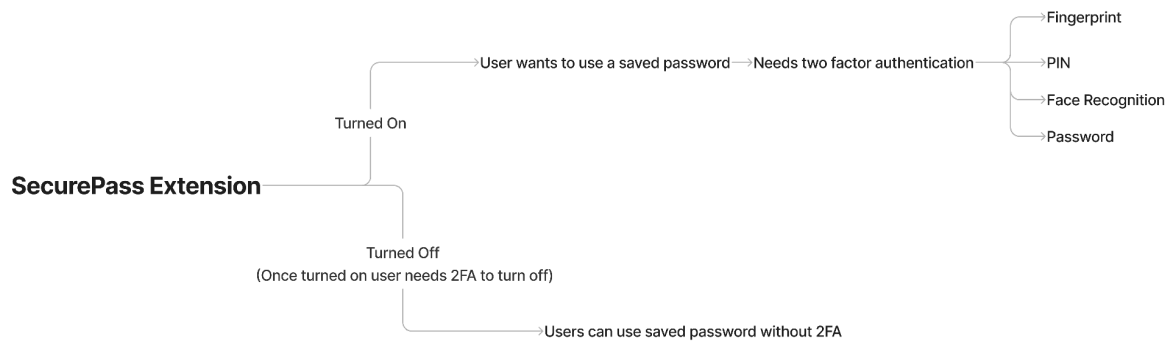
Already have an account, login?

If you want to use the saved password

Enter the Password

123

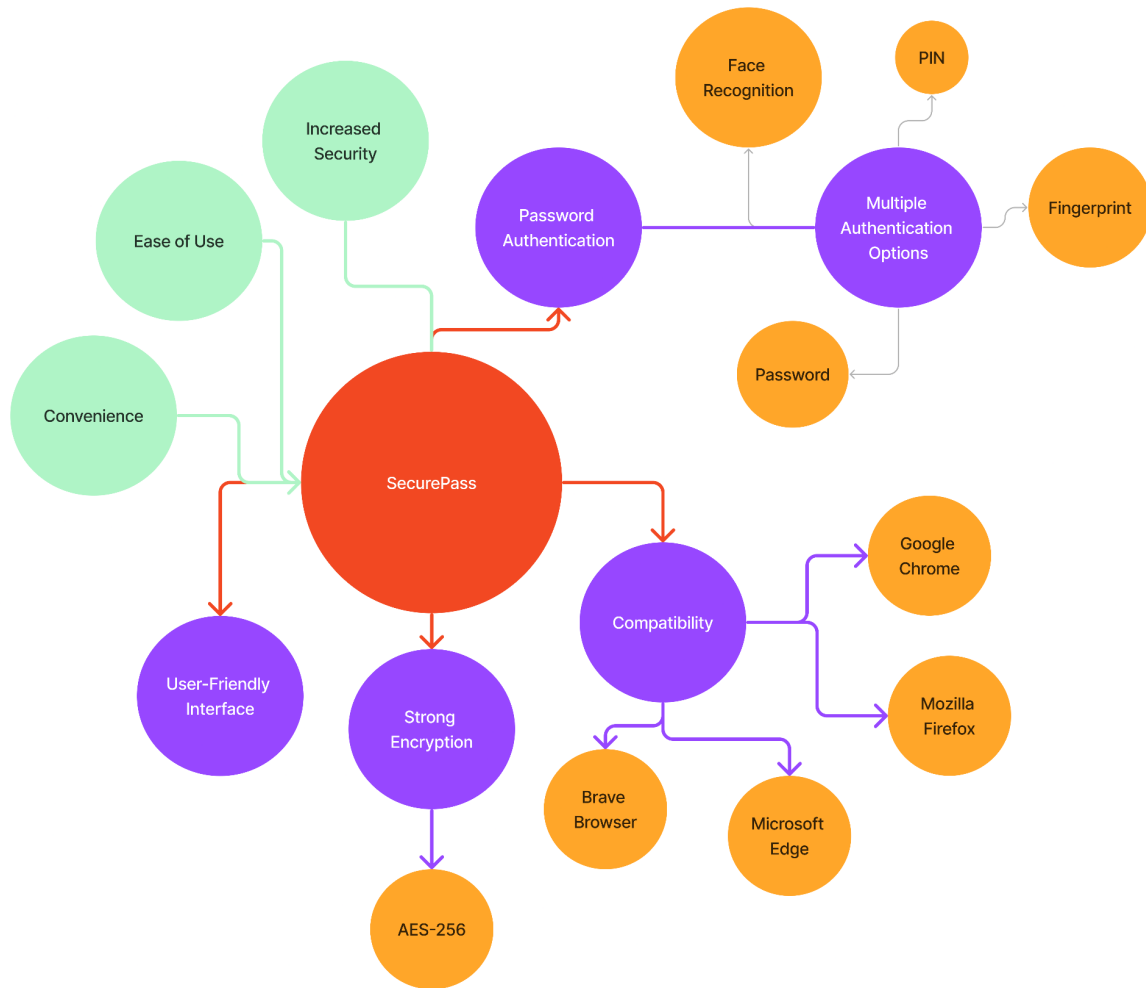
## Task flow ([Link](#))





---

## Findings ([Link](#))



### Features:

1. **Password Authentication** - With SecurePass, users must enter a password or use biometric authentication whenever they want to access their saved passwords. This will prevent unauthorized access to their accounts and protect their sensitive information.
2. **Multiple Authentication Options** - Users can authenticate themselves using a password, fingerprint, or facial recognition, making accessing their saved passwords more convenient.

3. ***User-Friendly Interface*** - SecurePass will have a user-friendly interface that is easy to use and navigate. Users can easily add, remove, and edit their saved passwords.
4. ***Strong Encryption*** - All saved passwords will be encrypted using AES-256 encryption, considered one of the strongest encryption standards.
5. ***Compatibility*** - SecurePass will be compatible with popular web browsers such as Google Chrome, Mozilla Firefox, and Microsoft Edge.

**Benefits:**

1. ***Increased Security*** - With SecurePass, users can be assured that their saved passwords are protected and can only be accessed by authorized users.
2. ***Convenience*** - SecurePass provides a convenient way for users to access their saved passwords without compromising security.
3. ***Ease of Use*** - SecurePass will have a user-friendly interface that is easy to use and navigate, making it accessible to all users.
4. ***Compatibility*** - SecurePass will be compatible with popular web browsers, making it accessible to a wider audience.