



Tribhuvan University
Madan Bhandari Memorial College
Kathmandu, Nepal

A Project Proposal
on
“Password Manager Extension for Google Chrome”

*A Project report submitted in partial fulfillment of the requirement for the degree
of Bachelor of Science (B.Sc.) Computer Science and Information Technology*

Submitted By
Sarita Sharma
Saumyata Nepal
Shubharaj Thapa
Yuvraj Sah

Submitted To:
Er. Ram Kumar Basnet
Department of Computer Science and Information Technology
New Baneswor, Kathmandu

2025

ABSTRACT

The proposed project focuses on developing a Password Manager Extension for Google Chrome, designed to enhance the user experience in managing online credentials securely. With increasing reliance on digital platforms, individuals face challenges in maintaining unique, strong, and secure passwords for multiple accounts. This extension aims to simplify this process by providing two primary functionalities Password Generation and Password Retrieval.

The extension leverages advanced encryption algorithms to ensure data confidentiality and employs multi-factor authentication for secure access. Its lightweight design integrates seamlessly with Google Chrome, enabling users to store, generate, and retrieve passwords with minimal effort. This tool not only reduces the risks of weak or reused passwords but also promotes safer digital practices.

By addressing the core needs of password management, the Password Manager Extension provides an efficient, user-friendly, and secure solution tailored for modern internet users.

OBJECTIVE

The objective of the **Password Manager Extension for Google Chrome** is to provide a secure and efficient way for users to manage their passwords directly from their browser.

The main objectives are as follows:

- 1. Enhance Security:**

Ensure users can generate and store strong, unique passwords using encryption techniques to safeguard sensitive data.

- 2. Simplify Password Management:**

Provide an intuitive interface for users to easily generate and retrieve passwords within the Google Chrome browser.

OVERVIEW

The Password Manager Extension for Google Chrome is a proposed solution aimed at addressing the challenges of managing online credentials effectively and securely. In today's digital landscape, where users often juggle multiple accounts across various platforms, maintaining unique and strong passwords is crucial for protecting personal and sensitive data. This extension simplifies the process of password management by integrating two essential features:

Password Generation:

- Automatically generates secure and complex passwords.
- Allows customization of password length and character composition (e.g., inclusion of uppercase letters, numbers, symbols).
- Provides users with the option to save the generated passwords securely in an encrypted format.

Password Retrieval:

- Enables users to retrieve stored passwords effortlessly through an intuitive interface.
- Ensures security by requiring user authentication, such as a Master Password or Two-Factor Authentication (2FA), to access stored credentials.
- Displays decrypted passwords only after successful verification.

The extension is designed with a user-friendly interface to provide a seamless experience while maintaining strong security standards. By employing encryption to store passwords and implementing robust authentication mechanisms, the tool ensures that user data is protected from unauthorized access.

Key benefits of the Password Manager Extension include:

- Simplified password management for multiple accounts.
- Elimination of weak or reused passwords, enhancing online security.
- Integration within Google Chrome for accessibility and convenience.

This extension is targeted at individuals and professionals who seek a reliable and efficient way to manage their online credentials. With this tool, users can navigate the complexities of modern digital security effortlessly and securely.

WORKFLOW PROCESS

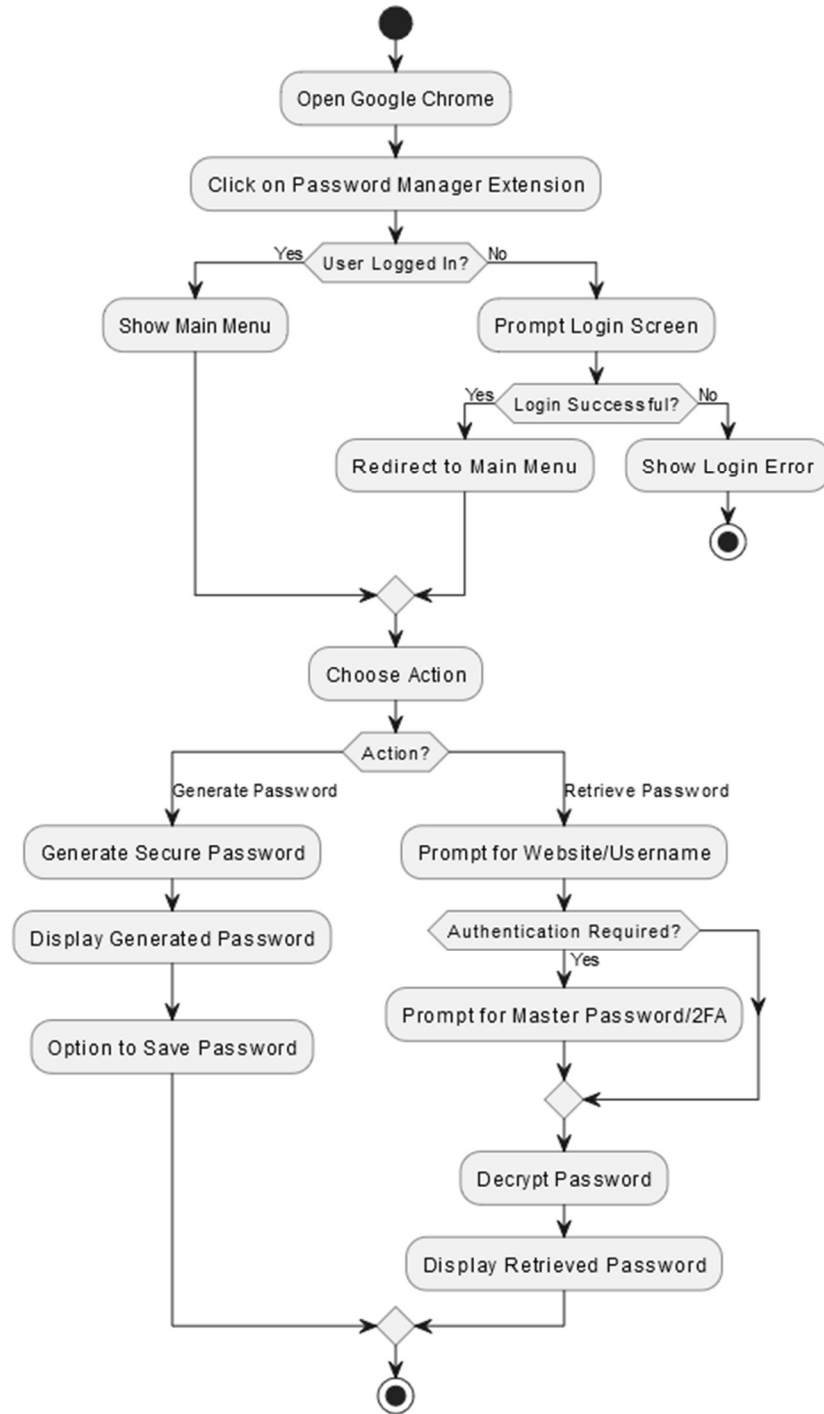


Fig : Workflow Diagram of Password Manager

Step 1: Accessing the Extension

Open Google Chrome and access the password manager extension.

Step 2: Login Check

Check if the user is logged in, and proceed to the main menu or prompt for login.

Step 3: Login Process

Prompt the user to enter credentials, and proceed to the main menu if successful, or show an error message if failed.

Step 4: Choose Action

Present the user with the options to generate or retrieve a password.

Step 5: Generate Password

Generate a secure password if the user selects "Generate Password" and offer an option to save it.

Step 6: Retrieve Password

Prompt the user for the website or username if "Retrieve Password" is selected, and decrypt the password after authentication.

Step 7: End Process

End the process by allowing the user to either exit or log out of the extension.

Conclusion

The proposed Password Manager Extension for Google Chrome offers an efficient and secure solution to address the challenges of managing online credentials in the modern digital landscape. By integrating features like password generation, secure storage, and retrieval, the extension simplifies the process of maintaining strong, unique passwords for multiple accounts.

The use of advanced encryption techniques and multi-factor authentication ensures that user data remains secure and protected from unauthorized access. Furthermore, the seamless integration with Google Chrome and a user-friendly interface enhances accessibility and convenience for users.

This tool not only empowers individuals to adopt safer digital practices but also contributes to reducing the risks associated with weak or reused passwords. As reliance on digital platforms continues to grow, the Password Manager Extension stands as a critical tool for promoting a more secure and efficient online experience.