JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Enhancing Password Manager Chrome Extension through Multi-Authentication and Device Logs

Karthika Venugopal K,
6th Semester – MCA Department
Jain University – School of CS and IT

Prof. Priya. N
MCA Department
Jain University – School of CS and IT

Abstract

People used to have a few passwords for a few critical web programs that you used to shop, study, remain connected, and get work done once upon a time, during the early years of the Internet. Things are a lot trickier now. According to the 2017 research from Last-pass, users had to remember an average of 191 distinct passwords—just for work—not to mention their own passwords. With the use of the proposed system, users can store their credentials in an organized manner such as Finance, Shopping, OTT, social media, Work. Users can also add to their own categories. In addition to that while logging in, the user needs to go under 2FA verification where a unique six-digit numeric code will be sent to the user's registered Email ID and track about devices which are active in his profile settings.

Keywords: *Password manager, Authentication,2FA, Chrome Extension, unauthorized access.*

Introduction

This Proposal for Password manager product will be an open-source product that is a cross-platform application that involves PGP Encryption standards & users need to submit their digital signatures related files to access their profile every time they need to manage their passwords. Another impeccable feature of this product is to provide users easy accessibility through cross-device authentication. At initial stages of this project development, planning to implement this project idea as a Google Chrome extension later based on the user's feedback improvise the idea in the future as a Desktop Application / Mobile Application.

1.1 Aim of the Project

The main motive behind this project is to provide user with a secured password manager in the form of google extension which can accessed anywhere & in any google web store supported browser & provide users with a list of device logs represent the number of devices the account is active in.

1.2 Scope

The Significance of the proposed system is to provide users a secure password manager by overcoming below cons of the existing Chrome extension(Existing System).

- Cross-Device authentication.
- Digital Signature for Recovery and Backup of account.
- PGP Encryption and Decryption standard to store & retrieve users data.
- Multi-factor authentication is implemented to improve the initial security of the application.
- Device logs are made available to the user so that the user can keep track of which device is active & which is not.

1.3 **Problem Statement:**

- The available password managers are either Desktop Applications or Web Apps. So every single time a user needs to launch the application & update the password manager database if there's any change made to the credentials.

- All the available password manager extensions use AES/DES encryption/decryption standards so passing through those encryption keys is not a tedious task for hackers.

Literature Survey

1. A different technique of authentication is to use devices that are always nearby and personal like mobile phones or a credential server. Password-based authentication protocols are the result of a lot of research and testing. Wu suggests using a strong password , more contemporary protocols such as the PAKE protocols, can function with weak passwords to prevent dictionary attacks on the information transferred. When compromising a service provider, different variants of PAKE protocols prohibit an attacker from impersonating a user . CompactPAKE is a protocol that is similar to EKE2 however, it is more compact and incorporates user key parameter retrieval as well as asymmetric authentication .

2 The PAKE authentication mechanism is used by Better Auth, although it doesn't support password stretching . Van Laer proposes using KDF for password stretching and storing the needed salt parameters at the service provider , which is similar to our method. In comparison to our work, they only use pre-defined KDF factors, such as CPU cost, and only have configurable salt, making their account aging solution inflexible. They also employ the Schnorr protocol , which is susceptible to parameter attacks, such as when the provider provides a tampered salt value.

3 An intriguing Key Derivation Function strategy is that it is not susceptible to parameter attacks . When assessing a Halting Key Derivation Function, the user runs a KDF algorithm until it reaches a halting parameter. A password that isn't legitimate can't be ruled out completely. When attempting a dictionary attack, this results in an attacker having to do more than three times the work . The HPAKE authentication protocol employs an HKDF and saves the necessary halting parameter at the predefined provider . External attackers can't see the halting parameters because of a covert credential retrieval technique , which makes offline dictionary attacks unfeasible. A parameter attack would be impossible with HPAKE since the user's HKDF calculation would not finish. A usability issue with HKDFs is that a user who inadvertently enters an erroneous password does not receive a timely notification about the error. Any typical state-of-the-art KDF can be used with our method.

4 Another set of authentication techniques makes use of external devices such as mobile phones or a credential server . No additional device or server is required in our job for the service provider's authentication. Management of passwords. A method that does not require the use of a server. A user's password being reused on several websites is to deduce a hash function that takes the value of the authentication key as inputs, passes the domain name and the password . Since this method is sensitive to dictionary assaults. To strengthen the hash function, it was recommended to use it n times.is the password n, on the other hand, is a hard-coded value. This indicates that the method will not be adaptable to future hardware.

5 Pvault provides two prominent services like cloud storage and password management, with the drawback of using the same password for both data encryption and storage server authentication. Zhao uses KDF to protect a password that is stored on a secure, reliable cloud storage system, but a simple authentication technique is used. Passport uses a similar basic key stretching mechanism as Halderman, except KDF parameters are stored on a Passport server. Passport, on the other hand, uses the Secure Remote Password protocol for authentication, which is vulnerable to parameter attacks.

6 The contributing factors of research carried out in the field of password manager has had a direct impact on cryptography and penetration testing. Hence, the majority of this study focuses on vast collections of academic studies on the security measures taken by most featured password managers and penetration testing experiments performed by security auditing teams. Furthermore, any checks performed on password managers have been extended to the full extent possible.

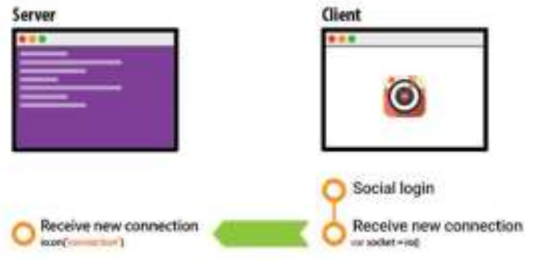
7 Moving on to the security analysis trends, we learned about featured password manager services like LastPass and 1Password. Auto-fill is a function present in several popular password managers, and other browser based password managers like Chrome web browser and Safari web browser. It has been discovered that major flaws exists that takes advantage of the auto-fill feature, such as iFrame sweep attacks, password sync exploits, and injections.

PROPOSED SYSTEM ARCHITECTURE

Proposed System Architecture

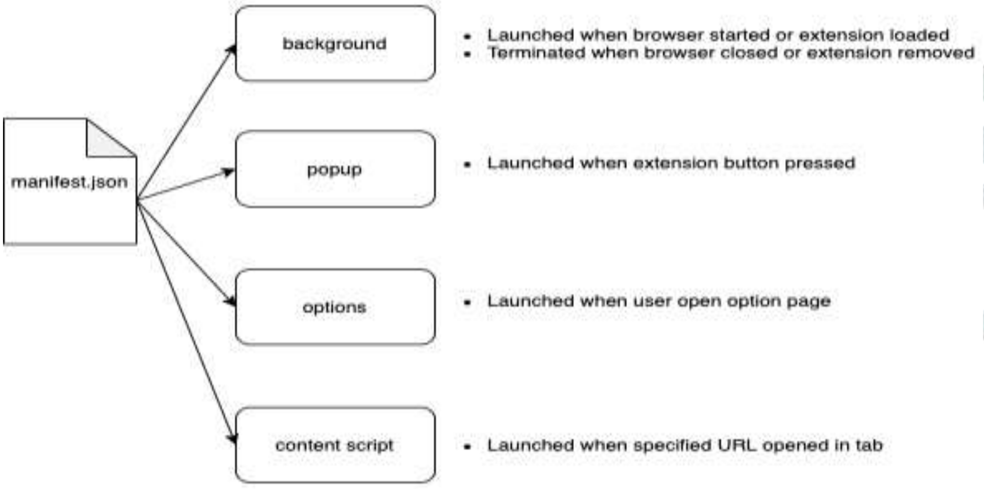
The proposed system will be an open-source and cross-platform application that involves PGP Encryption standards. Users are required to submit their digital signature related files to access their profile every time they need to manage their passwords. Another impeccable feature of this product is to provide users easy accessibility through cross-device authentication.

Architecture

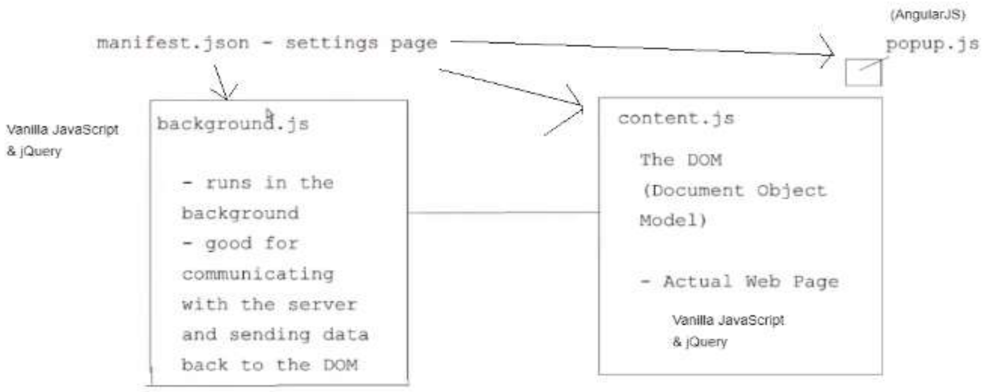


The above diagram shows the relationship between server & client and how the function of a client is dependent on the server for the functioning of the product.

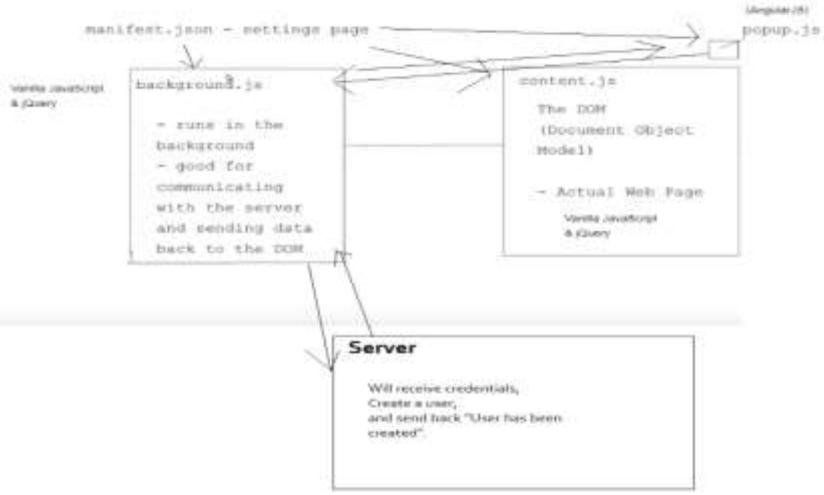
Structure Of the Extension


manifest.json
background
Launched when browser started or extension loaded
Terminated when browser closed or extension removed
popup
Launched when extension button pressed
options
Launched when user open option page
content script
Launched when specified URL opened in tab

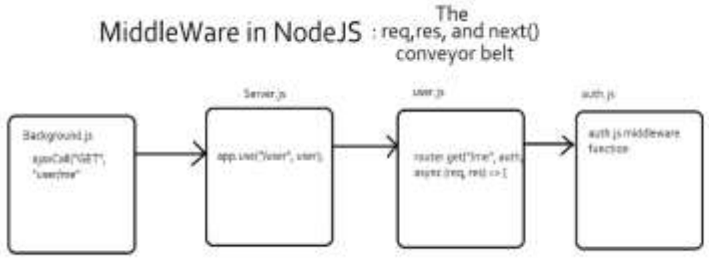
Chrome extension Structure



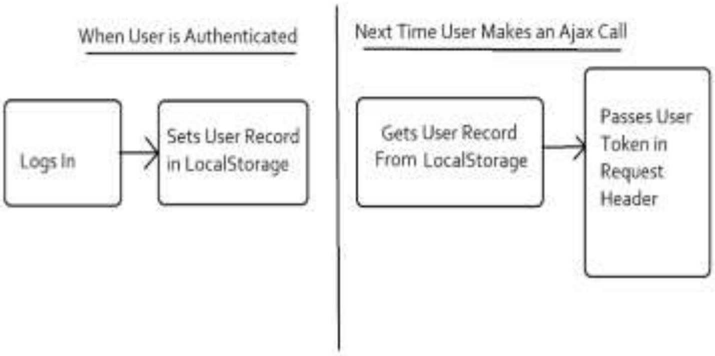
Authentication flow architecture



Node.js middleware flow diagram



Local Storage & User token generation process



CONCLUSION

We introduced an improved password manager approach as a Google Chrome extension in this study. We demonstrated that secure password-based encryption utilizing PGP encryption technology requires a strong authentication approach that maintains the users password confidential. To authenticate, users would just require their login credentials and decrypt their data with the suggested system, which allows them to save their passwords in an organized manner.

REFERENCES

- M. Bishop and D.V. Klein. Improving system security via proactive password checking. Computers & Security, 14(3):233–249,
- J. Bonneau. The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. Security and Privacy (SP).IEEE Symposium on, pages 538–552, 2012.
- D. Malone and K. Maher. Investigating the distribution of password choices. In Proceedings of the 21st international conference on World Wide Web, WWW "12, pages 301–310, New York, NY, USA, 2012. ACM
- https://www.thirdrocktechkno.com/blog/node-js-socket-io-chrome-extension-integration/
- https://ieeexplore.ieee.org/document/8456009
- https://ieeexplore.ieee.org/document/8326801
- https://www.section.io/engineering-education/speakeasy-two-factor-authentication-in-nodejs/#:~:text=May%205%2C%202021&text=Two%2Dfactor%20authentication%20is%20a,username%2Femail%20and%20password%20authentication.