Browser-Based Password Manager Using Tokenization

Teoh Xin Pei[1], Intan Farahama Binti Kamsin[2], Zety Marlia Zainal Abidin[3], Hemalata Vasudavan[4]
[1'2'3'4]Asia Pacific University of Technology and Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia.
[1]teohxinpei@gmail.com, [2]intan.farahana@staffemail.apu.edu.my, [3]zety@staffemail.apu.edu.my, [4]hemalata@staffemail.apu.edu.my

Abstract **- The browser built-in password manager makes it simply for user to manage their password credential. The purpose of this research is to propose a cloud-based browser password manager with using the browser extension and aim to achieve a high level of security. This study will employ data tokenization function to save password credential data. The methodology of the study will be carried out using survey and stratified sampling. Moreover, the target user will be those who using browser. In conclude. The research paper would be discussing the security of the browser password manager including the build-in and third-party extension and the reason of implementing the tokenization technique into the browser password manager. The future research for this proposed system is where implementing the 2FA or OTP feature to replace the manually entering if master password.**

Index Terms **- Browser build-in password manager, Password manager extension, Tokenization**

1. Introduction

The password manager providing the service of creating, storing, deleting and auto-filling password into the specified application for user. The majority of the user tend to re-apply the password across the other website due to the convenient and easy to remember. Yet, with the convenience of password manger, the user began to implement stronger and longer passwords and keep the password credential in the password manager without concern of memorizing it. In fact, with the research of [1] do confirm that the password manager help the user reduce the duplicating password across the several website. Oftentimes, the browser such as Google Chrome, Mozilla Firefox, Edge and Opera will pop-out a prompt to ask the browser user whether to save the password, that is browser built-in password manager. Thru, it is one of the best approaches to assist users better manage their website password credentials [2]. The browser built-in password manger stores the password in the database cloud with applying various type of encryption, include SHA-1, AES-256, 3DES and OS [3].

2. Literature Review

2.1 Research Domain

2.1.1 Browser Password Manager

Browser password manager divided into two type which is browser build-in password manager and Brower extension password manager. According to [3] who did an extensive study on password manager security stated that most of the browser built-in password manager rely on the device's operating system to encrypt the password vault. Therefore, by stealing the user mobile devices the attacker is able to obtain the password vault [4]. Based on the research of [5] and [6] had proposed a similar technique to protect the password vault by using the hashing technology such as SHA 256 that provide one way process that is non-decryptable. Yet, the research of [7] had launched an attack where the SHA 256 hashing can be attacked in 277.8 millisecond with 16 length of input. Nonetheless, the superiority of [5] researcher is where it implemented the zero-knowledge protocol, high secure cryptography which make the password vault more secure.

Moreover, the study of [3] mentioned that the majority of browser extension password managers do not support synchronization, which is one of the issues that leads to the user reusing the password. On top of that, the LastPass password manager supports synchronization, and the researcher [8] successfully exploited the LastPass password manager's extension permission by importing the malicious extension into the browser that contained the consolidation techniques, resulting in the LastPass extension successfully consolidating with the malicious extension.

As the [7] proofs that the hashing techniques does not secure as expected and the browser built-in password manager has an extremely weak password vault that can easily be attacked. Therefore, in this research the security of password vault and synchronization of the password manager will be in concern and be solve by using tokenization vault and isolating the extension correctly to prevent the malicious extension attack. The zero-knowledge protocol will be implemented to the tokenization vault in order to increase the security of vault.

2.1.2 Tokenization

Tokenization is the process of replacing confidential data with non-sensitive token data, which are a string of numbers with the same format as the confidential data, but no significance and de-tokenization is the process of returning the tokenized confidential data [9]. Yet, the de-tokenization can only process by the original tokenization system [10].

Moreover, there is two-type of tokenization service which is centralized tokenization and distributed tokenization [10]. In the distributed tokenization service where the token requestor (TR) can be generated in various token server provider (TSP), which the process is faster than the centralized tokenization service that required the TR generate the token through the only TSP. The TSP provide the service of tokenization, de-

tokenization and validation of the token data integrity and origination token and validation with cryptograms [11].

Additionally, there is three-type of which is word tokenization that splitting the confidential data into one piece of word, character tokenization that splitting the sensitive word or sentence into one piece of alphabet and sub-word tokenization that splitting between the word and character [12]. Based on the research of [9] stated that with the open-source sub-word tokenizer, SentencePiece, it help to develop the end-to-end and language independent system.

Moreover, based on the research of the tokenization technique [13] had implemented in various market and most the countries government such as Argentina, Iran and Spain had also utilized the tokenization techniques to store the assets into database. Based on the journals that has been written [14] [11] [10], the tokenization framework had widely implemented in the online e-wallet payment. The [4] had proposed a password management with using tokenization as the decoy password. Therefore, it shows that the tokenization techniques are secure as it implemented in the online payment [4].

As the tokenization is mainly utilized in the online payment, therefore it shows that the tokenization method is way secure. As in the present browser password manager, most of the password database is utilizing encryption method instead of tokenization method. In short, the tokenization method of saving browser password credential with the sub-word tokenizer and decentralized tokenization service will apply in this proposed system.

2.2 Similar System

2.2.1 1Password

1Password is a password manager application which support the operating system including Mac OS, iOS, Windows, Android, Linux and Chrome OS. Additionally, the 1Password password manager offer the packages for personal, family, business, and teams [15].

Figure 1: Logo of 1Password[15]

In term of the safety and privacy of the user's password confidential, 1Password has implementing the AES-256-bit encryption techniques to save the password credential into the password vault. Moreover, PBKDF2-HMAC-SHA256 had applied for key derivation which makes it harder for attacker repeatedly guess the password. The 128-bit secret key had applied and act as another level of security and it is created on the user's devices, thru the 1Password have no right to access and record it. The purpose of the secret key is to protect the password credential off the user's devices, and it used to combine with the user's password credential that had been stored in the 1Password [15].

Figure 2: Example of secret key in 1Password [15]

The 1Password secures the user's password credential with a master password and the master password can verify with using the two-factor authentication (2FA) and biometric access. Therefore, the user would just need to remember the master password in order to unlock the other application's password. On top of that, the 1Password having the password generator that suggest the user with a stronger password that contain 34-character [16].

Beyond that, 1Password offer the outstanding feature that difference than other password manager which is travel mode, emergency kit, and watchtower. The watchtower vulnerability alert notifies the user when the website has been hacked. The emergency kit feature is useful when the user forgotten the master password as this feature will be provided when the user first sign in. The travel mode is useful when the user had lost the devices, the 1Password will lock the devices password vault [17].
On top of the extension feature, based on the review of the 1Password user on Firefox browser [18], the extension would needs to run simultaneously with the 1Password application and the synchronization in the browser extension is not stable enough.

2.2.2 RoboForm

The RoboForm is a password manager software application and it support the feature of browser extension along with the synchronization. The operating system that the RoboForm supported such as Windows, Mac, iOS, Linux and Android. Moreover, the RoboForm provide the package of personal, family and business [19].

Figure 3: Logo of RoboForm [20]

On the subject of saving password credential in the cloud password vault, the RoboForm encrypt using the AES256 bit encryption with PBKDF2 SHA256, 4096 iterations in all stages. On top of that, the decryption process will be held on the local devices, therefore the decryption key will never hit to the RoboForm server [21].

In the security concern, the master password is encrypted with the secret key and the master password will not be saved into the RoboForm server, instead, it will be saved in user's local devices. The master password of the RoboForm is encrypt using the AEX, BlowFish and 3DES encryption. Nonetheless, in case the user had forgotten the master password, the RoboForm admin could help to reset the master password. The RoboForm also allow the provide the multi factor authentication option

such as two factor authentication (2FA) and one time password (OTP) which adding extra layer of protection to the RoboForm account. It also provides the generate unique password feature and audit the user's password strength feature. Additionally, the user can enable the biometrics or touch ID feature in order to login into the RoboForm [20].

Moreover, the RoboForm also provide the online auto filling checkout form. In such, the user will have to predefine the details of the information in the RoboForm application and when navigate to the website that required the user to fill up the identity form, the user will just have to click on the button for auto filling [22].

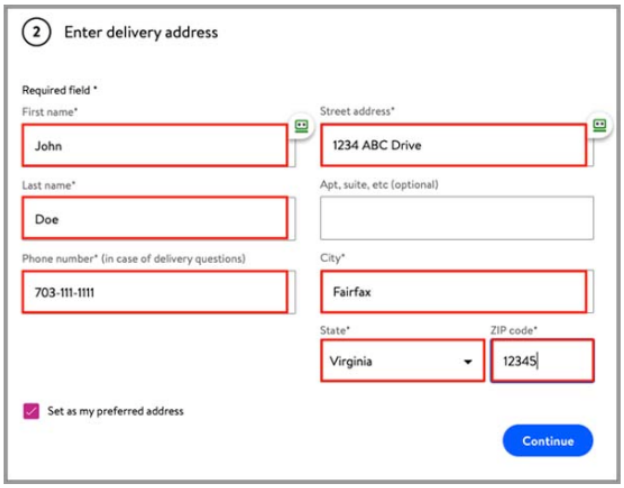

Figure 4: Online Auto Filling Checkout Form [22]

2.3 Comparison Table

Features	1Password	RoboForm	Proposed System
Synchronization within Browser	Yes	Yes	Yes
Auto Generate Password	Yes	Yes	No
Auto Filled Password	Yes	Yes	Yes
Extension	Run simultaneously with application	Run simultaneously with application	Manage password credential via extension
Way to Verify Master Password	2FA and password	2FA, OTP via email and SMS and password	Password
Encryption for password credential	AES 256-bit, 128-bit secret key and PBKDF2-HMAC-SHA256 key derivation	AES256 bit Encryption with PBKDF2 SHA256, 4096 iterations	Sub-Word Tokenizer and Decentralized Tokenization Service
Special Feature	Travel Mode, Emergency Kit, and Watchtower	Online Auto Filling Checkout Form	None
Targeted Customer	Personal, Family, Business and Team	Personal, Family and Business	Personal
Supported Operating System	Mac, iOS, Windows, Android, Linux, and Chrome OS	Windows, Mac, iOS, Linux and Android.	None, user will manage through browser extension
Browser Extension Supported	Safari, Firefox, Chrome, Brave and Microsoft Edge.	Major browsers, including Microsoft Edge, Google, Bing, Yahoo and Firefox	Safari, Chrome, Firefox and Microsoft Edge
Pricing	14-day free trial and paid [15]	14-day free trial and paid [20]	Free

3. Problem Statement

An interview had been carried out by [23], most of the user who utilized the browser-based password manager were motivated by convenience and unaware of the threat. Yet, as mentioned in the study by the [5], the encrypted password stored by the browser-based password manager are vulnerable and easy to attack, which the attack can decrypt the password and logging into the victim account without entering a master password in Firefox and Opera. Based on another research that had been driven by [3], majority of the browser password managers, including as Chrome, Firefox, and Opera, save the password in an *SQLite* database, which is a local data storage for particular application. The encryption used by the Chrome and Opera is an Operating System (OS) encryption whereas the Firefox browser storing and encrypting the password with Secure Hash Algorithm 1 (SHA-1) and Triple Data Encryption Algorithm (3DES) [3]. It proved by [8] which conducted a research-based exploit that targeted and attacked Chrome built-in password manager and LastPass Chrome Extension, a well-known third-party password manager application, by utilizing *Spook.js* under the Ubuntu operating system. As a result, as demonstrated in the research, *Spook.js* successfully leaked the credential auto filled by the Chrome password manager without needing any user action, whereas LastPass only decrypts

passwords when credentials must be filled into a website while keeping all usernames in memory in readable text [8].

4. Research Aims and Objectives

4.1 Aim

The aim of this study is to safeguard the user's password credential and allow the user to manage and preserve their password on a web browser in a secure environment by utilizing a third-party extension.

4.2 Objective

i. To design the third-party password manager extension to store the username and password.

ii. To implement a data tokenization service to store the browser password.

iii. To allow users to synchronize their passwords across devices by storing the password credential in a cloud database.

iv. To allow user to access the password credential that had been stored in the password manager extension through master password

5. Research Significance

The findings from this research would make some contributions to the browser environment's password management as it will reduce the chance of password credential being leaked and pwned. Additionally, it also helps the user memories those difficult and strong password. With this browser password manager, the user can create a stronger and longer password without affair of forgetting the password. Yet, even if the tokenization vault being leaked, the attack will only get the tokenized password credential, which carry no meaning. Therefore, by using this browser password manager, it can reduce the user using the reused password.

6. Methodology

7.1 Sampling Method

This study will use the stratified sampling method of probability sampling since the data will be collected through a survey and disseminated throughout the Klang Valley zone. Therefore, it will be huge number of respondents. With the stratified sampling, the research is able to manage the distribution of a survey sample in terms of factors that define the strata as the data will be collected and divided into smaller group based such as concern of browser password manager and manually memorized password [24]. As stated by the study of [25], the stratified sampling method provide permit meaningful subgroup analyze. Therefore, with implementing the stratified sampling, the research can inspect collected data's attribute of browser password manager in a more effective and visualize way.

7.2 Identify Respondents

Users who use the browser without utilizing a password manager or who use a password manager, such as the browser's built-in or a third-party extension password manager, are the target audience for this survey. Google Chrome, Mozilla Firefox, Safari, Microsoft Edge, and Opera are among the browsers available. By getting this targeted audience's feedback, it can help this project in term of what are the audience main concentrated on, is either the password security or the convenience of the password manager.

7.3 Data Collection Method

In this study, the researcher will be conducted a survey, and the number of targeted audiences will be 100 and will be conducted based on Klang Valley zone. The questionnaire will be distributed by using the self-administer method, which the questionnaire will be sent out through using the email, social media such as Instagram, Facebook and WhatsApp. The questionnaire will be divided into 3 sections and approximate 10-question will be developed and the survey will be collected in a closed-ended question with 5-point Likert scales, yes and no. The 3 sections include the general basic information such as gender and age, the behavior of storing password and the attitude toward the browser built-in password manager. By conducting the survey, the researcher may understand the audience's account security, current password behaviors in term of will the audience reuse the password to the other website, and the opinion toward to password manager. All in all, before handling the questionnaire out to the audients, the researcher will be carried out a pilot test in order to assure the quality of the questionnaire through the criterial of, is the question that had been asked is easy to understand, straightforward and is the researcher will get the expected answer from the audients.

7. Overview of the Proposed System

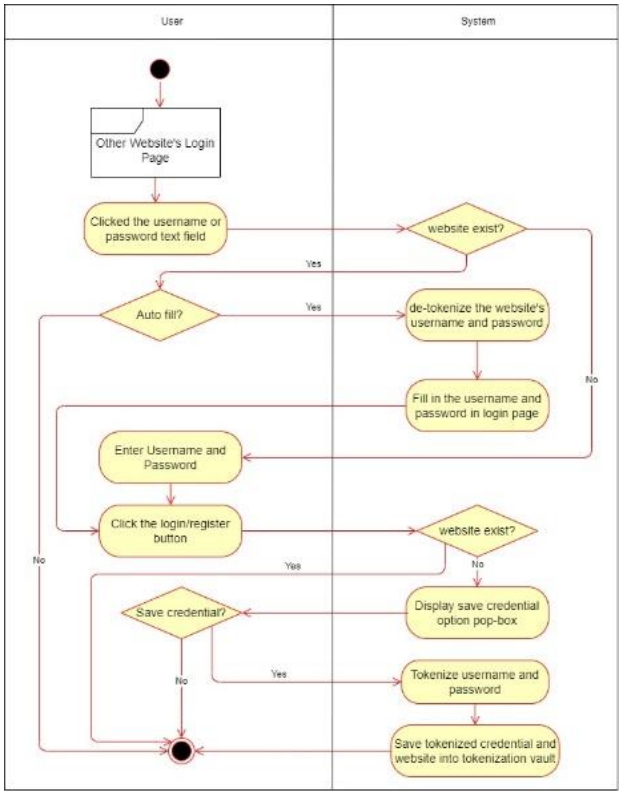

Figure 5: Activity Diagram for Tokenization Password Manager

Figure 5 show that the activity diagram for the password manager by using the tokenization techniques to create and save the username and password in the tokenization vault. While the password manager system detected that the user is visiting the login page, and the cursor is clicked the text field of username or password, in backend system will check is the website URL exist. If yes, the system will appear the option pop box for user to allow the user to choose whether to allow the password manager system to auto fill up the password. If the user chooses to use the password manager's password credential the backend of the system will de-tokenize the tokenize password credential and help the user to fill into the textfield. After the system help to input the password, the user is required to click the button and the system will check is the website exist in the vault again. If no, the system will ask is the user wanted to store the password into the tokenization vault. Once the user clicks yes, the system will tokenize the password credential and save it into the vault.

8. Conclusion

All in all, the according to the research that had been conducted, it show that the hashing and encryption method can be easily to attack, which this encryption method is highly utilize in the browser build-in password manager. Therefore, the proposed browser password manager will implement the tokenization technique to store the password credential into the cloud password vault. With the cloud password vault, the user is able to synchronize the password across the devices. On top of that, it also helps the user to prevent reused password across the other website platform. In term of the future research, instead of accessing the password credential via entering the master password manually, the system could implement the OTP or 2FA feature as acted as another layer of the security.

References

[1] S. G. Lyastani, M. Schilling, S. Fahl, M. Backes, and S. Bugiel, "Better managed than memorized? Studying the Impact of Managers on Password Strength and Reuse," p. 19, 2018.

[2] S. Oesch and S. Ruoti, "That Was Then, This Is Now: A Security Evaluation of Password Generation, Storage, and Autofill in {Browser-Based} Password Managers," 2020, pp. 2165–2182. Accessed: May 03, 2022. [Online]. Available: https://www.usenix.org/conference/usenixsecurity20/presentation/oesch

[3] T. Oesch, "An Analysis of Modern Password Manager Security and Usage on Desktop and Mobile Devices," p. 187, 2021.

[4] H. Bojinov, E. Bursztein, X. Boyen, and D. Boneh, "Kamouflage: Loss-Resistant Password Management," in *Computer Security – ESORICS 2010*, vol. 6345, D. Gritzalis, B. Preneel, and M. Theoharidou, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 286–302. doi: 10.1007/978-3-642-15497-3_18.

[5] R. Oladipupo and A. Olusola Olajide, "An Enhanced Web Security for Cloud-based Password Management," Jun. 2019.

[6] A. Hossain, H. Rahaman, A. Jamil, and M. Khan, "An Algorithm for Securing User Credentials by Combining Encryption and Hashing Method," vol. 03, pp. 2600–9633, Oct. 2020.

[7] D. M. A. Cortez, A. M. Sison, and R. P. Medina, "Cryptographic Randomness Test of the Modified Hashing Function of SHA256 to Address Length Extension Attack," in *Proceedings of the 2020 8th International Conference on Communications and Broadband Networking*, Auckland New Zealand, Apr. 2020, pp. 24–28. doi: 10.1145/3390525.3390540.

[8] A. Agarwal *et al.*, "Spook.js: Attacking Chrome Strict Site Isolation via Speculative Execution," p. 17, 2022.

[9] T. Kudo and J. Richardson, "SentencePiece: A simple and language independent subword tokenizer and detokenizer for Neural Text Processing." arXiv, Aug. 19, 2018. Accessed: May 17, 2022. [Online]. Available: http://arxiv.org/abs/1808.06226

[10] W. Liu, X. Wang, and W. Peng, "State of the Art: Secure Mobile Payment," *IEEE Access*, vol. 8, pp. 13898–13914, 2020, doi: 10.1109/ACCESS.2019.2963480.

[11] M. Bosamia and D. Patel, "Wallet Payments Recent Potential Threats and Vulnerabilities with its possible security Measures," *Int. J. Comput. Sci. Eng.*, vol. 7, pp. 810–817, Jan. 2019, doi: 10.26438/ijcse/v7i1.810817.

[12] J. He *et al.*, "ChEMU 2020: Natural Language Processing Methods Are Effective for Information Extraction From Chemical Patents," *Front. Res. Metr.*

Anal., vol. 6, 2021, Accessed: May 06, 2022. [Online]. Available: https://www.frontiersin.org/article/10.3389/frma.2021.654438

[13] N. Ebrahimiyan, M. L. Ghahroud, S. B. A. Abadi, and F. Jafari, "Tokenization and its application in different countries," *J. FinTech Artif. Intell.*, vol. 1, no. 1, Art. no. 1, Jul. 2021.

[14] P. Janulek, "Tokenization as a Form of Payment and Valuation Professional, Scientific, Specialist and Technical Activities," *SSRN Electron. J.*, Jan. 2018, doi: 10.2139/ssrn.3307180.

[15] 1Password, "About your Secret Key," *1Password*. https://support.1password.com/secret-key-security/ (accessed May 17, 2022).

[16] 1Password, "Pricing & free trial," *1Password*. https://1password.com/sign-up/ (accessed May 17, 2022).

[17] 1Password, "About the 1Password security model," *1Password*. https://support.1password.com/1password-security/ (accessed May 17, 2022).

[18] Firefox Browser Add-ons, "1Password – Get this Extension for Firefox (en-US)." https://addons.mozilla.org/en-US/firefox/addon/1password-x-password-manager/ (accessed May 17, 2022).

[19] RoboForm, "Browser Extensions – RoboForm." https://help.roboform.com/hc/en-us/categories/203879667 (accessed May 18, 2022).

[20] RoboForm, "Key Features," *Everything you need to manage your passwords*. https://www.roboform.com/key-features (accessed May 17, 2022).

[21] RoboForm, "Security – RoboForm." https://help.roboform.com/hc/en-us/categories/203877668 (accessed May 18, 2022).

[22] RoboForm, "Online checkout forms: form filling from an Identity," *RoboForm*. https://help.roboform.com/hc/en-us/articles/115005691207-Online-checkout-forms-form-filling-from-an-Identity- (accessed May 18, 2022).

[23] S. Pearman, S. A. Zhang, L. Bauer, N. Christin, and L. F. Cranor, "Why people (don't) use password managers effectively," p. 20, Oct. 2019.

[24] X. Zhao, J. Liang, and C. Dang, "A stratified sampling based clustering algorithm for large-scale data," *Knowl.-Based Syst.*, vol. 163, pp. 416–428, Jan. 2019, doi: 10.1016/j.knosys.2018.09.007.

[25] Y. Tang, "MOVER confidence intervals for a difference or ratio effect parameter under stratified sampling," *Stat. Med.*, vol. 41, no. 1, pp. 194–207, Jan. 2022, doi: 10.1002/sim.9230.