

Improving the privacy of Facebook users through browser plugin

MSc Internship
MSc in Cybersecurity

Cho Fai Bartholomew Cheung
Student ID: x18192807

School of Computing
National College of Ireland

Supervisor: Mr. Niall Heffernan

National College of Ireland
MSc Project Submission Sheet
School of Computing




Student Name: ...Cho Fai Bartholomew Cheung.....
Student ID: ...x18192807.....
Programme: ...MSc in CyberSecurity..... **Year:**2021.....
Module: ...Academic Internship.....
Supervisor: ... Mr. Niall Heffernan
Submission Due Date: ...16th August, 2021.....
Project Title: ...Improving the privacy of Facebook users through browser plugin.....
Word Count:6412..... **Page Count:**.....18.....

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature: 
Date:15th August, 2021.....

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	<input type="checkbox"/>
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	<input type="checkbox"/>

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Improving the privacy of Facebook users through browser plugin

Cho Fai Bartholomew Cheung
X18192807

Abstract

Facebook is the most popular online social media in the world, its users all over the world. The users can connect with their families, friends, and colleague, etc, and share their personal information, live photos, video, and feeling via Facebook. However, most Facebook users do not aware that their privacy is misused by Facebook without their consent, Facebook may even disclose its user's data to third-party organizations. Currently, there is no privacy and security preservation mechanism in online social media and notify the users clearly that their data may be used by Facebook or third-party organizations. In this paper, the solutions and recommendations from the researchers for improving Facebook user privacy will be studied and analyzed. Moreover, a browser plugin (or extension) will be studied for the possible solution to enhance the privacy of Facebook users in this research, the users can be aware of their privacy in Facebook and how the plugin can protect their data.

1 Introduction

Nowadays, most people live a busy life and they do not have time to learn about the recently from their friends and families directly. Therefore, they keep connections with others via online social media instead of traditional methods, such as phone conversations or meetings. There is a huge number of online social media in the world, the famous media include Facebook, Twitter, Instagram, and Snapchat, etc. They provide a handy and user-friendly interface for their users to share anything with anyone in their friend lists, including their recent live, feeling, photos, video, and locations, etc. Due to convenience, the users share their sensitive information to the online social media unconsciously. Then, their information will be at risk of being used improperly. Especially Facebook has the most users in the world. In most cases that the information will be used as an advertisement by Facebook, and in the worst case, it will be involved in a crime by a criminal.

In this paper, a brief description of the literature reviews will be mentioned, all of them are valuable for plugin design, and the possible way to develop the plugin, the summary of the literature review will be at the end of this section. The suitable tools to develop the plugin are also introduced in this paper, and the structures with the workflow will be mentioned as well. The last, what the Facebook users could do to protect their data, and the feasibility of using a plugin in the Internet browser for users to protect their data during the users are using Facebook.

As Facebook is a very famous online social media in the world, a huge number of people use this media to keep in touch with others, but they don't aware that Facebook and third-party apps are using their data without their consent and most of them disclose their private

information inadvertently in Facebook. Therefore, they must understand the importance of their data being safe and what happens if their data is not well protected. Moreover, they need to know how to make their data safer when using Facebook, also a technology could be able to help them to improve the privacy, plugin of the browser will be proposed for the improvement.

2 Literature Review

As Facebook is the most popular online social media in the world, so a lot of people pay attention to personal data privacy when using Facebook, and some people studied how to improve privacy. There are a lot of methods to improve privacy. This section introduces the literature review from researchers for the Facebook privacy studying.

2.1 Browser extension

Most of the authors use browser extensions to improve Facebook privacy for Facebook users. Rishabh Khandelwal et al [1] used to leverage the fine-tuned encoder to develop a browser extension for Facebook users to search the privacy setting by free form queries, it solved the reachability issues of the privacy settings. And then, it can save time and effort for the users to find the privacy settings. The authors developed the user interface by Chrome browser extension which is supported by a natural language query interpreter. The users can search for privacy settings via the interpreter. With back-end server support for the extension, the user can find the related setting by semantic matching. The user interactions are handled by the client-side for showing the query results from the server. The extension will provide a basic list interface when the icon is clicked and display the privacy settings of the specific field. Callum Pilton et al [2] designed a Google Chrome Extension as well and it is called Paradox, it provides the three wireframe designs for improving Facebook privacy, includes tracking and privacy policy-specific information are showing in a different method. It also has popup designs for the summative policy analysis, the users could have 2 different ways to check the policy analysis. And it has a user-friendly design for "full report" and "report privacy violation", both have the same banners for the users to read easily by the pages are spitted into sections of related details.

Leucio Antonio Cutillo et al [3] develop a FaceCloak as a Firefox browser extension for Facebook privacy. They used JavaScript to implement AES for encrypting and decrypting the Facebook content and using SHA-1 for indexing the encrypted data, the length of all keys is 128bits. FaceCloak has 2 useful tools for users to share the key to others via e-mail easily. The first tool is an e-mail list manager, it provides a contact list for the users to add e-mail addresses on it for their friends. Another tool is created on the Facebook page dynamically, it is used for adding a new friend. Privacy protection for the Facebook Wall and Facebook Notes applications are also supported by the extension for preventing data disclosure happened by Facebook. Kevin Tang et al [4] also developed a Firefox browser plugin called "NOYB" for encrypting the Facebook user's profile by adding a button in the Facebook pages. The page can be decrypted by another button that is added to another user's page. The authors created a dictionary for the plugin and post it on a public website for the users to inquire anonymously. The user needs to enter the password for the encryption and decryption. The key can send to the friends automatically via the plugin and return the keys from friends via webmail.

2.2 PriSEC

Rishabh Khandelwal et al [5] built a privacy settings enforcement controller to find, display, and deploy the Facebook privacy settings for enhancing the accessibility of the privacy controls. The controller calls PriSEC and using machine learning techniques. PriSEC has a 3-stage pipeline for a specific domain to extracting a machine-readable representation of its privacy controls. PriSEC uses the machine learning classifier to identify the privacy control page, which uses the text and UI functions of the website. Then, PriSEC interacts with all UI elements on the page to simulate users' behaviour and the elements could be classified into types by a deep-learning-based visual classifier.

2.3 Facebook Privacy Pudges

Yang Wang et al [6] designed 2 types of nudges for Facebook users to have better decisions to share their information on Facebook, but neither of them is not able to restrict the users to post anything to Facebook. The first nudge is an Audience Nudge, it is based on the existing privacy setting of the post to show 5 profile pictures that are chosen randomly from the pool of people who can view the post. Those pictures divided into different groups of people, such as family members, friends, colleagues, and etc for the users to recognize the relationship easily, and let the users decide who can read their sharing. Another nudge is a Timer Nudge, it is used to providing some time to the users to think before sharing on Facebook. After the users pressed the "post" button on Facebook, the post won't be shared immediately, the users will have 20 seconds to cancel the sharing, so they will have enough time to consider sharing the information or not.

2.4 Visibility Visualization Tool

Stan Damen et al [7] used Prolog in Facebook's privacy controls to make the users' information visible, based on the users' privacy settings and tagging. The developed tool is used for improving the users' awareness of the risk for privacy disclose and let the users can control their details.

2.5 User-friendly Interface

Heather Richter Lipford et al [8] developed the audience view interface for privacy setting interface by copying the static HTML from different Facebook profile pages. The interface can make a specific Facebook user can be found from searching, networks, friends, or themselves only. Then, the users can decide who can see their sharing by the privacy settings, but not just the privacy menus which Facebook provides. Another author Thomas Paul et al [9] had an Improved Interface Design for a new interface and integrate it into the Facebook page, it could reduce the possible cognitive issues. The main menu is under the profile picture with an attractive link, the link can redirect the page to the configuration page for privacy setting modification. A colouring scheme is applied to the modified mode for reading all current privacy settings easily. Each of the coloured buttons can change the privacy settings of related profiles.

2.6 Education

Alexa Stein et al [10] made 3 categories of videos, each of them is consistent with interventions used in education. Fear Appeal: this category of videos makes the users scary via the potential privacy issue, then the users will understand the result if they do not protect their information properly; Reflective Learning: this category of videos make the users reflect on their decisions and actions they did in the Facebook, it makes the users have better decisions and actions in the future if they did anything is not good in the past. A Reflective Learning approach produces a positive result for the users, then they will learn from past

mistakes and improve them in the future. The videos may make the users regret the past sharing as they disclosed their privacy and make them change their attitudes and behaviours when using Facebook.

2.7 Privacy-By-Proxy

Adrienne Felt et al [11] used API to develop an application that can transform the third-party output by a website. They aimed to protect the users' identification and provide applications that they had surveyed the identified capabilities, the application can show the friends' details and traverse the social graph. The application can show the user details to the Facebook users who have the right to read. It can protect the users' details, but third-party applications need to access the social graph information in the users' friend list directly, this is achieved by a user and graphic anonymous. And the application can limit access to normal public information to reduce the risk for exposing anonymized user identities during the public information is accessing.

2.8 Recommendation to Facebook

Some authors provide recommendations for Facebook to improve the privacy of Facebook users. Michelle Madejski et al [12] recommend Facebook to provide information tags feature for obtaining settings for unexpected features. Suggest automation of information categorization feature can help to manage a large amount of data. The information categories identified automatically successfully in the study by a primitive text search algorithm. Besides, some recommendations for the liberal nature of the algorithm, including machine learning, natural language processing, or image analysis technique. Shah Mahmood [13] recommends Facebook has to request its' users to provide their real names on the e-mail addresses, but not providing the real name to the users for confirmation. Then, the malicious users cannot get the users' real names from Facebook by using the users' e-mail addresses; Facebook should not show the mutual friends list to the users if they do not want their friends to see what friends they have on Facebook. Facebook should request the users to provide their identity such as passport and driving license to resume their account when they forgot their password, or their accounts are not accessible.

2.9 Access control scheme

Jun Pang and Yang Zhang [14] used a hybrid logic to define access control policies for an OSN model which have users and public information to improve Facebook user privacy. They based on public information to define several policies and formulated the policies with their proposed logic. Their logic was extended and become more practical by using category relations or relationship hierarchy and public information. Besides, unreliable information and collaborative access control in OSNs could be handled by extending their model and logic.

2.10 Safebook

Leucio Antonio Cutillo et al [15] recommend a decentralized OSN which is based on a P2P architecture, it could solve the problem for basic security and privacy, and the lack of trust and incentives via leveraging on the real-life trust of each user. It could be achieved by preserving the online social network application "Safebook". It contains a three-tier architecture, which has a direct mapping of layers to the OSN levels. The three-tier architecture including the SN level of the OSN

which is implemented by the user-centered social network layer; AS services which are implemented by the P2P substrate; the internet for the CT level.

2.11 Facebook wizard

Yabing Liu et al [16] developed privacy wizards to improve privacy, the wizards can infer communities by using machine learning algorithms. And the wizards can help users create friend lists easily on Facebook. The friends of the Facebook users can be grouped into communities automatically by the social link between the users for managing the privacy and a friend list can be made for each community of the friends.

2.12 flyByNight

Matthew and Nikita [17] developed a Facebook application "flyByNight" to reduce the privacy risks of using Facebook, the application can use client-side JavaScript to encrypt and decrypt important information. It can make sure the unencrypted information will not transfer to the Facebook servers, the servers will not keep the readable information and private key, and the information will not show on the Internet. The social network friend relationships are allowed to be managed by Facebook, and the key is managed in the Facebook interface.

Various approaches to improve privacy in Facebook from the literature, are creative and valuable for reference. They could be in a technical way or non-technical way, and they could be classified into 3 categories. The first category is education/ recommendation for Facebook or Facebook users; the second category is using application or plugin to make the privacy setting attractive and changing easily, the third category is using browsers' plugin to encrypt and decrypt the data when using Facebook. The approaches in the first category are easiest to implement as no programming is requested. The approaches in the second category require an application to support giving a convenient way to the user adjust the privacy setting, but it can follow the privacy mechanism of Facebook only, does not fully protect the user's data privacy. The approaches in the third category are the most complicated, as encryption and decryption are involved in these approaches, but they are the best way to protect the user data.

3 Research Methodology

This research was based on collecting information from the literature (such as article journals, books, and conference proceedings, etc) to study the research questions and developed a suitable tool to solve the problem from the research questions as the title mentioned. Datasheets and numbers were not involved in this research, only the textual information from the literature was used. Therefore, qualitative data was used in this research, the data can be described textually but not numerically. Moreover, all data were used in this research came from the study, the observations, and the experiment, etc from other researchers and literature reviews. So, the research used secondary data as the data source. And then, descriptive research was used to collect the data without affecting the study objects. The qualitative analysis method was used for this research, the analysis was performed through analysed the textual information from literature reviews, the information could come from a survey, interviews, case studies, etc, but the information was not involved any numbers.

The proceed of the research is shown in the following figure:



Figure 1: Proceed of research.

Firefox browser extensions were developed by authors Leucio Antonio Cutillo et al [3] and Kevin Tang et al [4] to improve the Facebook user privacy when they are using Facebook, all of them using encryption to protect the privacy data, and Advanced Encryption Standard (AES) was used for encryption and decryption of both extensions, the message could be read by anyone who has the valid key, the Facebook users use the specific key to encrypt the message and post to the Facebook, they can share the key to their friends. Then, only their friends can read the message, but Facebook can only read the meaningless message. Encryption is the possible solution to improve privacy when using Facebook, and it could combine with other functions to enhance the usage. Improve the Facebook user view interface was emphasized by authors Heather Richter Lipford et al [8] and Thomas Paul et al [9], different colours were used for different privacy setting of Facebook can attract the Facebook users attention on the privacy settings, so the colourful interface can attract the Facebook users attention.

According to the information gathered from the literature review, the data is encrypted before posting to Facebook is the safest way to protect the user data for Facebook users, then Facebook and its third-party partner cannot access the data without the valid key to read the data. Facebook users can share the key with their families or friends to decrypt the message with the Firefox extension (or plugin) to read the message. The visual reminder should be provided to the Facebook users that when they are using Facebook, so the extension will create a red border automatically when the users are browsing Facebook websites, and the users will be reminded their data may be disclosed and they need to use the Facebook Privacy Tool to encrypt the message before sharing in the Facebook.

Regarding the encryption method, AES encryption is used for the Facebook Privacy Tool, as another 2 tools FaceCloak [3] and NOYB [4] also use AES encryption for their Firefox browser extensions. Galois Counter Mode of AES (AES/GCM) is used because it is the most used encryption mode for data protection. GCM has 2 independent features, one is for authentication (GMAC), the other one is for encryption. This mode uses CTR mode to perform the encryption, and the GHASH function (128-bit binary) is used for Message Authentication Code (MAC) generation. The recipient can check the MAC value before the decryption for the integrity of the message to make sure the message security. Other encryption modes cannot fulfil the same criteria as GCM. It can be a stand-alone MAC, even the data does not need to encrypt but still perform the authentication without modifications, because all lengths of the initialization vectors (IV) could be accepted by GCM, then the applications would be easier to fulfil the various requirement of IV [18]. AES-GCM is the famous encryption algorithm in Authenticated Encryption with Associated Data (AEAD), it does not encrypt the specific part of the message and transfer it as that part of the message treat as associated data. AES-GCM is still used to encrypt the network packet even with no encryption for the associated data, because it still can use to verify the data integrity and authenticity. Up to now, Transport Layer Security (TLS) and the National Institute of Standards and Technology (NIST) authentication encryption standard (SP 800-38D) uses AES-GCM for authentication encryption [19].

To avoid the password is decrypted by hackers, advanced cryptographic functions are used to protect the password. The most common method to keep the password safe is hash-based schemes, Password-

Based Key Deviation Function 2 (PBKDF2), bcrypt, and scrypt are the popular Password Hashing Schemes (PHSs). The only standardized construction for the RFC 2898 and the RSA Laboratories' PublicKey Cryptography Standards (PKCS) is PBKDF2 in PHSs [20]. PBKDF is a type of key derivation function, it uses a pseudo random function (PRF) to generate a secure key from the input values of users, includes user-defined password, iteration count, and salt. PBKDF has 2 versions. PBKDF1 (PBKDF version 1) uses Message Digest 5 (MD5) or SHA-1 as its PRF, but both have security issues that were found by many researchers. This version of PBKDF is replaced and only used for compatibility with old applications. Therefore, PBKDF2 (PBKDF version 2) is used to solve the problems of PBKDF1 and recommended for keys generation by a password for secure system [21]. PBKDF2 generates the key from the password and the salt by Hash-based Message Authentication Codes (HMACs). The salt is a series of numbers up to 8 bytes, it can protect from rainbow table attacks which are using tables of hashes computed in advance, and dictionary attacks which are trying to find the password by the possible words. Therefore, PBKDF2 is used on the Facebook Privacy Tool for password protection.

4 Design Specification

This tool is implemented in a client desktop/ laptop with Windows operating system and developed by similar web-based technologies, such as HTML, CSS, and JavaScript. An Atom text editor is used to develop the tool, that is a free open-source text and code editor for different types of the operating system, it is developed by GitHub, and it supports embedded Git Control and JavaScript. The tool is developed in Windows 10 operating system (version 20H2) 64x environment with Intel Core (TM) i5 1.60Ghz CPU, 16GB DDR4 RAM, and Intel (R) UHD Graphics 620 graphic card.

The first function of the Facebook Privacy Tool is providing the attractive visible reminder for the Facebook users to pay more attention to their data when using Facebook, the process as the figure 2 with the steps.

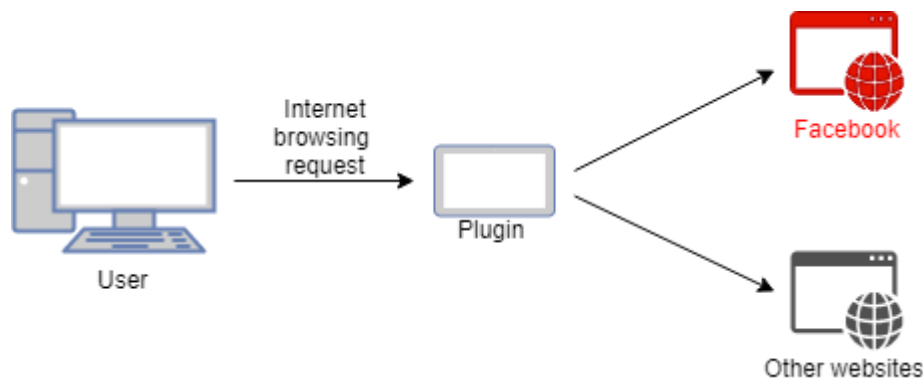


Figure 2: Red border for Facebook websites.

Process of the red border:

1. Users send internet browsing requests to the plugin (extension).
2. The plugin receives the request and base on the rule to add the red border to the browser or not.
3. The red border will be added around the browser if the users request to browse the Facebook website.
4. Nothing will be added around the browser if the users request to browse the websites other than Facebook.

The second function of the Facebook Privacy Tool is providing a perform to the Facebook users for data encryption and decryption, the users can decide the message that they want to share with the public without encryption or encrypt the message before posting the message for anyone who has the valid key to decrypt the ciphertext and read the message. The users need to enter the message to the tool with a key (password) for the data encryption and provide the key to anyone who they want to share to, the key can be shared by secure communication application, such as Signal or phone conference. The interaction of the plugin between the user's browser and the Facebook servers as shown in figure 3.

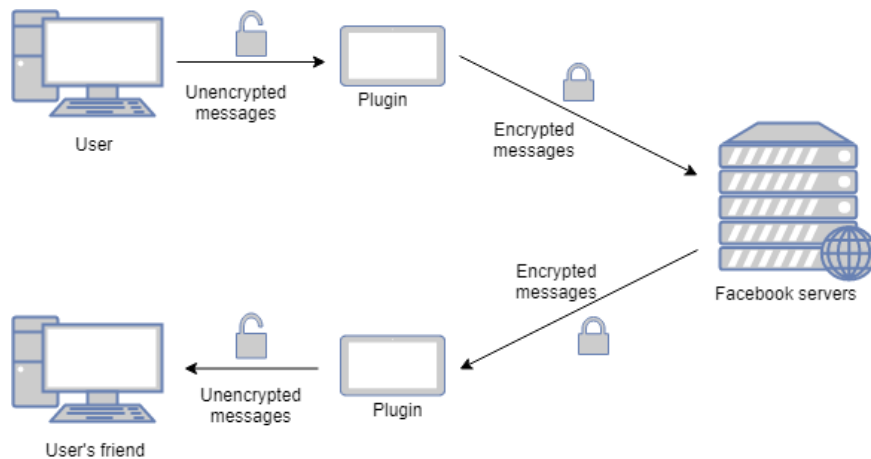


Figure 3: Basic plugin interaction.

The process of the data encryption and decryption are on the following:

Encryption:

1. Define a key (password) for generating the AES-GCM key for the data encryption or decryption
2. The key and a randomized salt value are used for the AES-GCM key generation.
3. The AES-GCM key is used to encrypt the message with a randomized initialization vector (iv).
4. The message will be encrypted by the AES-GCM key and a randomized initialization vector (iv).
5. As the decryption needs the values used for the key, iv, and salt for encryption, so base64 string is made for keeping the salt which was used to create the password-based key (PBKDF2), the iv which was used for creating the AES key, and the encrypted message. The key should not be disclosed.

Decryption:

1. The base64 string derives the encrypted message, iv, and the salt.
2. Create a PBKDF2 which is used to derive the AES-GCM key for encrypting or decrypting the message. Must use the same key as encryption.
3. Use the PBKDF2 key and the salt from the base64 string to create the AES-GCM key.
4. Use the AES-GCM key and the iv to perform the decryption for the encrypted message.
5. The encrypted message is decrypted to a readable message.

5 Implementation

The following figure 4 is showing the workflow of the Facebook Privacy Tool. Firstly, it will check the browsing website is Facebook or not. If so, the red border will be appeared around the browser to remind the users that they are using Facebook. If not, the users will browse the website as normal. And then if the users want to post a private message to Facebook, they can use the tool to encrypt the message and post to Facebook. Otherwise, they can post the message to Facebook directly.

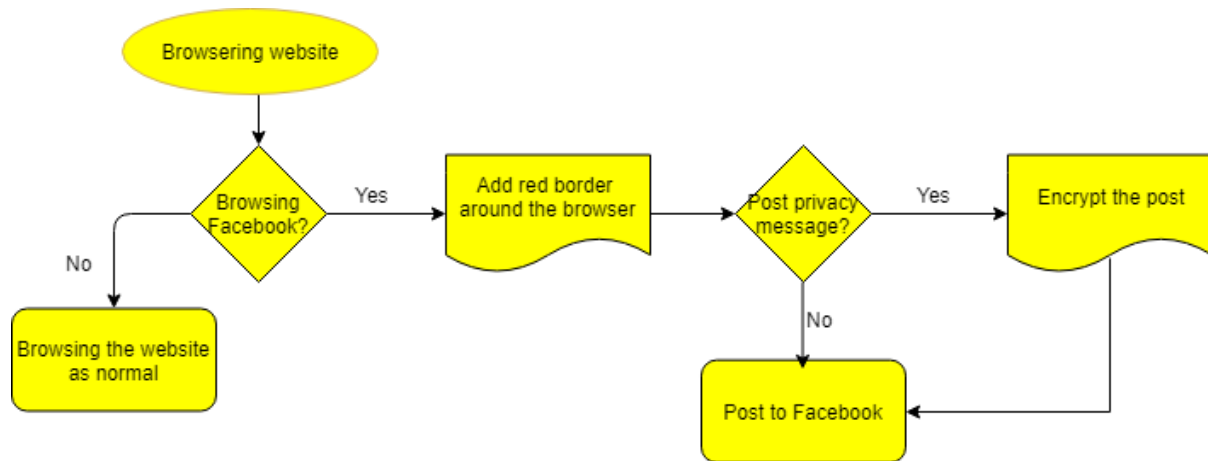


Figure 4: Facebook Privacy Tool workflow.

5.1 Visible reminder

A red border will appear around the browser when browsing the Facebook website, then it will attract the user's attention to keep an eye on their personal information when using Facebook.

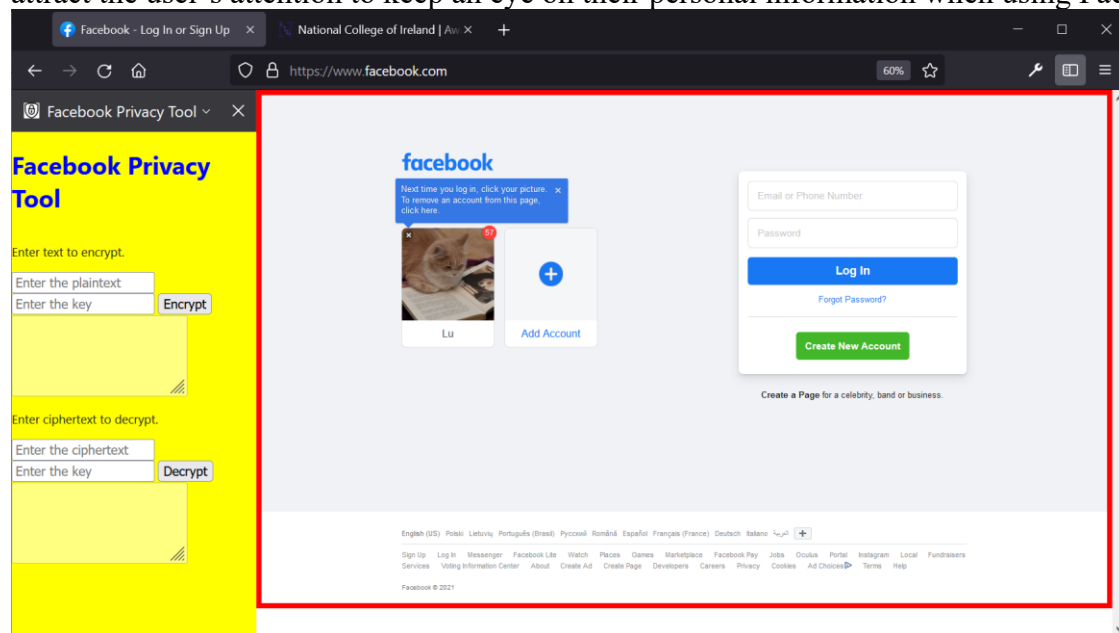


Figure 5: Red border around the browser.

5.2 Encryption

Input the message which wants to restrict the viewers to the first white box, define a key, and input to the second white box, then press the “Encrypt” button for the message encryption. The message will be encrypted successfully and prompt out the encrypted message, the users can copy the encrypted message and post it to Facebook. The key need to share the reviewers who do the users want them to read the message.

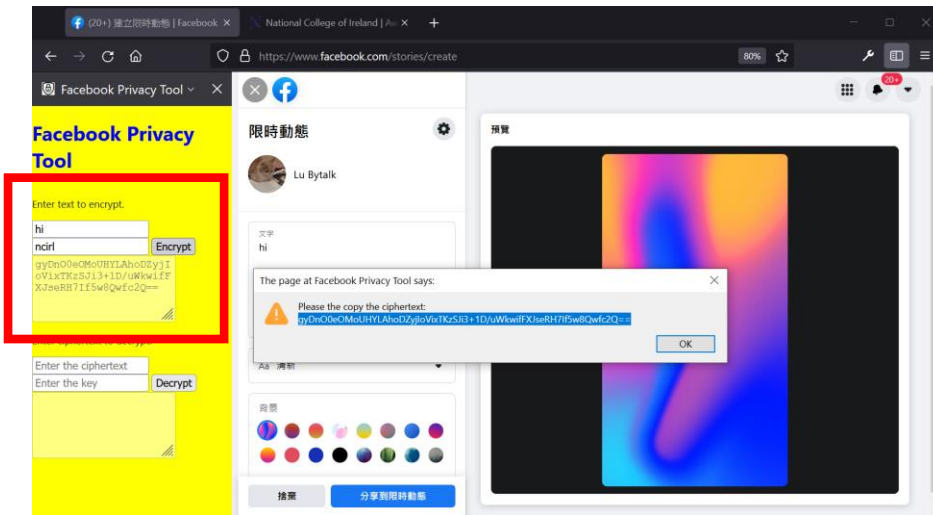


Figure 6: Encrypt the message and post to Facebook.

5.3 Decryption

The viewers input the encrypted message to the first white box under the sentence “Enter ciphertext to decrypt”, input the key which is provided by the users, and click the “Decrypt” button. Then, the encrypted message is decrypted and become a readable message.

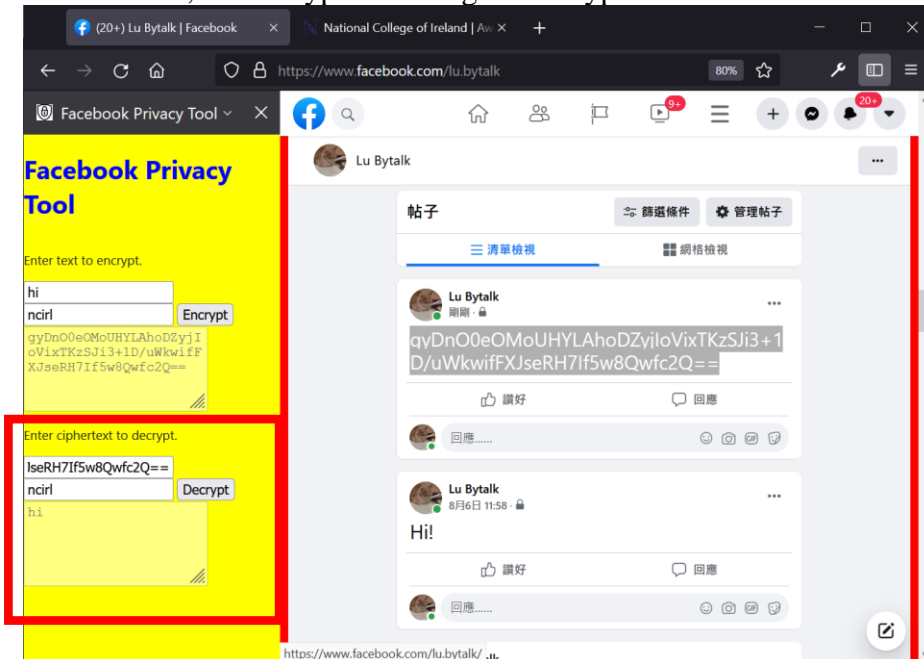


Figure 6: Decrypt the message and the message become readable.

6 Evaluation

The Firefox browser extension "Facebook Privacy Tool" was tested and evaluated on a laptop with Windows 10 operating system version 20H2, Intel Core (TM) i5 1.60Ghz CPU, 16GB DDR4 RAM, and Intel (R) UHD Graphics 620 graphic card. The software requirement is just Mozilla Firefox Browser version 91.0 (the latest version up to now). 3 parts of the extension were tested, including red border, message encryption, and message decryption. The testing details will discuss on the following:

6.1 Red border

The red border around the browser will appear when the users are browsing the Facebook websites as the figure 7. The red border won't appear when the users are browsing other websites than the Facebook website as figure 8.

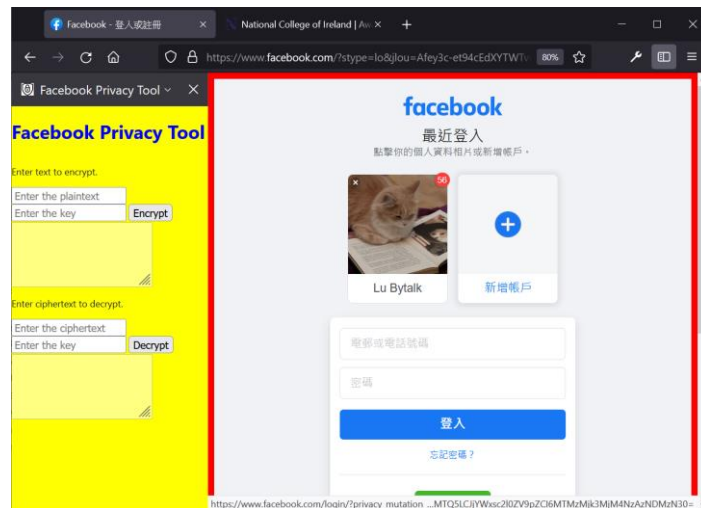


Figure 7: Red border for the Facebook websites.

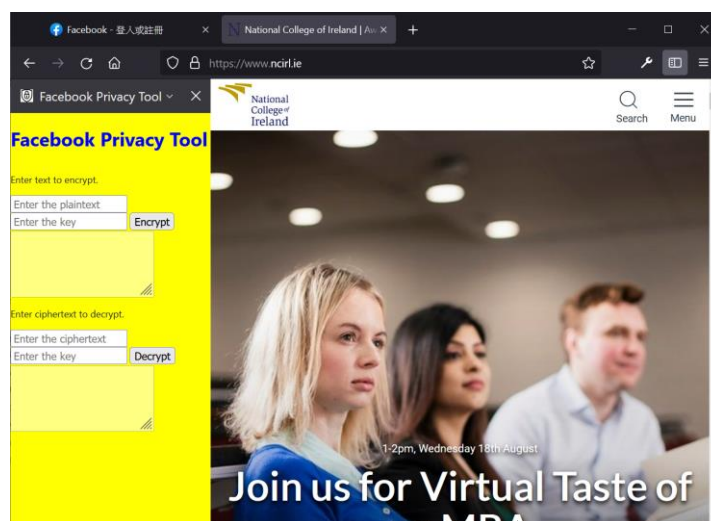


Figure 8: No red border for the other websites.

6.2 Encryption

The message “dublin” is encrypted by clicking the “Encrypted” button with the key “ncirl”, the result

“qgJK3AaiARMXd8GKF7KbHC8jtxL2b8ITO0hWxNrp1Ab5SBNwr8tEvdSPo3SdrXebSi4=” was prompted as shown in figure 9. As the password is protected by PBKDF2, even the plaintext and the key are the same, but the result is

“qgJK3AaiARMXd8GKF7KbHC8jtxL2b8ITO0hWxNrp1Ab5SBNwr8tEvdSPo3SdrXebSi4=” which is different from the previous encrypted message, the result as shown in figure 10.

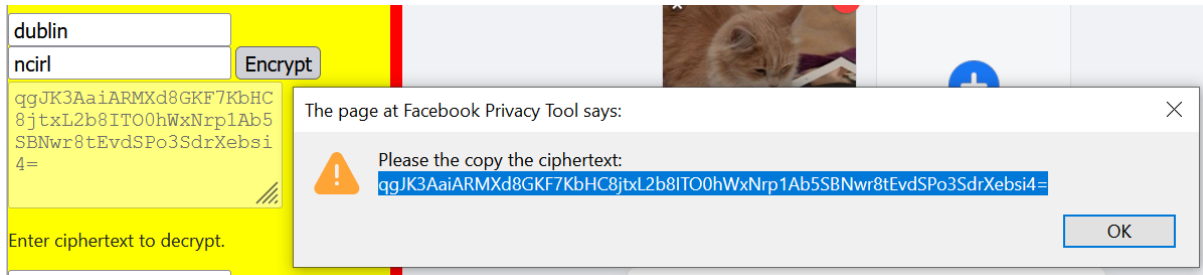


Figure 9: Message encrypted and prompt the result.

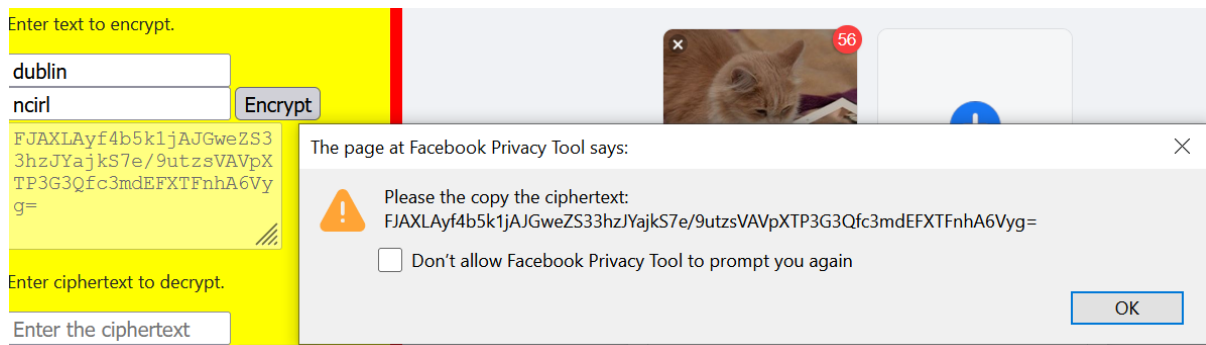


Figure 10: Same message encrypted with same key but different result.

6.3 Decryption

Both encrypted messages

“qgJK3AaiARMXd8GKF7KbHC8jtxL2b8ITO0hWxNrp1Ab5SBNwr8tEvdSPo3SdrXebSi4=” and

“qgJK3AaiARMXd8GKF7KbHC8jtxL2b8ITO0hWxNrp1Ab5SBNwr8tEvdSPo3SdrXebSi4=” can be decrypted to the original message “dublin” with the correct key as shown in figure 11 and figure 12. But if the encrypted message is incorrect, the decryption will be failed (as shown in figure 13), or the key is incorrect, the decryption will be failed as well as shown in figure 14. The result of the decryption will be shown as “Decryption failed”.



Figure 11: Decrypted the encrypted message to the original message.

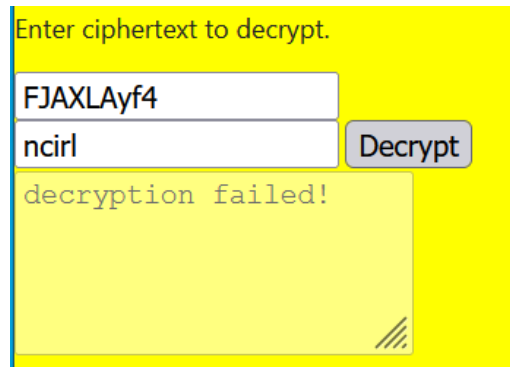


Figure 13: Decryption failed with the wrong encrypted message.



Figure 12: Decrypted the different encrypted messages and get the same original message.

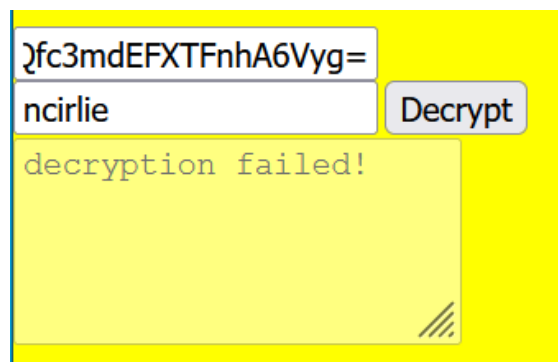


Figure 14: Decryption failed with the wrong key

According to the above test result, all functions of the Facebook Privacy Tool work properly. The first function red border appeared only for the Facebook websites; the second function encryption was able to generate an encrypted message with the key, the encrypted messages were different every generation of the message encryption, even the message and the key were the same; the third function decryption was able to decrypt both encrypted messages which were generated with the same message and key, and the decryption was failed if the encrypted message and the key were incorrect.

6.4 Performance testing

Performance is one of the critical factors for a successful application, even the application could provide perfect protection for the Facebook users' privacy, but the users won't use it if they need to wait for a long time for the application. Performance testing was done for the Facebook Privacy Tool, different situations were used for performance testing for encryption and decryption respectively. 10- and 30-characters' keys were used to encrypt 10-, 50-, and 100-characters' messages separately, the result of the test as shown in table 1. The encrypted texts from encryption performance testing were used to perform the decryption performance test with the same keys as used in the last test, the result of the decryption performance test as shown in table 2.

According to the testing results for both encryption and decryption below, the results were satisfied, the encryption and the decryption in a different situation could be done within 1s, it could be the acceptable time for any people to perform the encryption or the decryption.

Table 1: Performance of encryption

No. of key\No. of char.	10	50	100	150	200	300
10	0.73s	0.76s	0.81s	0.83s	0.91s	0.89s
30	0.77s	0.85s	0.78s	0.87s	0.93s	0.97s

Table 2: Performance of decryption

No. of key\No. of ciphertext	72	128	192	260	328	460
10	0.75s	0.87s	0.71s	0.78s	0.87s	0.91s
30	0.75s	0.74s	0.73s	0.74s	0.83s	0.93s

7 Conclusion and Discussion

In this research, many research papers were studied from other researchers, a lot of researchers studied the topic for Facebook privacy, their solutions to improve the Facebook users' privacy include using browser extensions in different platforms, attractive user interface, Facebook user education, and privacy setting recommendations for the Facebook. Synthesize the research results from the researchers, the encrypted message is the best method to keep the data private and avoid the data misused by Facebook or its third-party companies, and the attractive user interface can attract the Facebook users for their awareness of their data privacy. Therefore, the Facebook Privacy Tool was developed to improve Facebook users' privacy. The tool can display a red border around the Firefox browser to remind the users when they are browsing the Facebook website, and it provides the encryption/ decryption functions for the users to encrypt the message before post to Facebook and decrypt the message with the valid key. The user can use the encryption function with the Facebook privacy function to enhance their privacy, the users can set their posts to allow a specific group of people to view their post, even anyone has the valid key, but they still cannot see the post, as the users do not want them to see. The Facebook Privacy Tool is suitable for various types of Facebook users, anyone can use the tool with Firefox browser, even they are Windows or iMac operating system users. The performance of the tool is good for anyone, the encryption/ decryption can be done within 1 second. And the size of the tool is tiny, it just uses 5.84KB on the hard disk, almost does not use any space.

The Facebook Privacy Tool provides the essential functions for the Facebook users to protect their privacy, it still has some improvement in the future to provide a better user-friendly interface for the users, then the user can use the tool easier and efficiently. The encryption and the decryption functions could be embedded into the Facebook website. The users can enter the message into the posting box, the extension could be encrypting the message before post to Facebook, adding a rule to the extension for letting it knows which message need to encrypt, such as putting a symbol (e.g. &) to beginning and end of the message. If the message is without this symbol, then the message will be posted without any encryption. Besides, highlight the encrypted message on the Facebook website and the decrypted message will be prompted automatically. Therefore, the sidebar is not necessary to use the space of the browser. Asymmetric keys could be used instead of AES-GCM encryption, it provides better protection for the message, and It provides confidentiality, authenticity, and non-repudiation. The users do not need to remember the key and disclose it to other.

8 References

- [1] R. Khandelwal, A. Nayak, Y. Yao and K. Fawaz, “Surfacing Privacy Settings Using Semantic Matching,” *Proceedings of the Second Workshop on Privacy in Natural Language Processing*, no. 2020 Association for Computational Linguistics, p. 28–38, 2020.
- [2] C. Pilton, S. Faily and J. H. Bulmer, “Evaluating privacy - determining user privacy expectations on the web,” in *Computers & Security*, Science Direct, 2021, p. 102241.
- [3] W. Luo, Q. Xie and U. Hengartner, “FaceCloak: An Architecture for User Privacy on Social Networking Sites,” in *2009 International Conference on Computational Science and Engineering*, Vancouver, 2009.
- [4] S. Guha, K. Tang and P. Francis, “NOYB: Privacy in Online Social Networks,” in *WOSN '08: Proceedings of the first workshop on Online social networks*, Seattle, 2008.
- [5] R. Khandelwal, T. Linden, H. Harkous and K. Fawaz, *PriSEC: A Privacy Settings Enforcement Controller*, Vancouver, B.C.: USENIX Association, 2021.
- [6] Y. Wang, P. G. Leon, A. Acquisti, L. F. Cranor, A. Forget and N. Sadeh, “A Field Trial of Privacy Nudges for Facebook,” in *Proceedings of the SIGCHI Conference on Human Factors in Computing*, Toronto Ontario Canada, CHI '14, 2014, p. 2367–2376.
- [7] S. Damen and N. Zannone, “Privacy Implications of Privacy Settings and Tagging in Facebook,” in *Secure Data Management*, vol. 8426, Trento, Italy, Springer International Publishing, 2013, pp. 121-138.
- [8] H. R. Lipford, A. Besmer and J. Watson, “Understanding Privacy Settings in Facebook with an Audience View,” in *Proceedings of the 1st Conference on Usability, Psychology, and Security*, vol. 42, Charlotte, US, UPSEC'08, 2008, pp. 1-8.
- [9] T. Paul, D. Puscher and T. Strufe, “Improving the Usability of Privacy Settings in Facebook,” *ArXiv*, vol. 1109.6046, 2011.
- [10] A. Stein, N. M. Su and X. & Page, *Learning through Videos: Uncovering Approaches to Educating People about Facebook Privacy*, USENIX Association, 2020.
- [11] A. Felt and D. Evans, “Privacy Protection for Social Networking Platforms,” in *Web 2.0 Security and Privacy*, Oakland, The European Network and Information Security Agency, 2008.
- [12] M. Madejski, M. Johnson and S. M. Bellovin, “The Failure of Online Social Network Privacy Settings,” Department of Computer Science, Columbia University, New York, 2011.
- [13] S. Mahmood, “New Privacy Threats for Facebook and Twitter Users,” in *2012 Seventh International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, Victoria, 2012.
- [14] J. Pang and Y. Zhang, “A new access control scheme for Facebook-style social networks,” in *Computers & Security*, Elsevier, 2015, pp. 44-59.
- [15] L. A. Cutillo, R. Molva and T. Strufe, “Safebook: A privacy-preserving online social network leveraging on real-life trust,” *IEEE Communications Magazine*, vol. 47, no. 12, pp. 94-101, 2009.
- [16] Y. Liu, K. P. Gummadi, B. Krishnamurthy and A. E. Mislove, “Analyzing Facebook Privacy Settings: User Expectations vs. Reality,” in *IMC '11: Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, New York, 2011.

- [17] M. M. Lucas and N. Borisov, “flyByNight: Mitigating the Privacy Risks of Social Networking,” in *WPES '08: Proceedings of the 7th ACM workshop on Privacy in the electronic society*, New Yor, 2008.
- [18] P. K. Das, N. Sinha and B. Annappa, “Data Privacy Preservation Using AES-GCM Encryption in HEROKU Cloud,” no. EasyChair, p. 2615, 2020.
- [19] K. Kim, S. Choi, H. Kwon, H. Kim, Z. Liu and H. Seo, “PAGE—Practical AES-GCM Encryption for Low-End Microcontrollers,” *Applied Sciences*, vol. 10, no. 9, p. 3131, 2020.
- [20] Y. Luo, Z. Su, W. Zheng, Z. Chen, F. Wang, Z. Zhang and J. Chen, “A Novel Memory-hard Password Hashing Scheme for Blockchain-Based Cyber-Physical Systems,” *Association for Computing Machinery*, vol. 21, no. 1533-5399, p. 2, 2021.
- [21] H. Choi and S. S. C., “Optimization of PBKDF2-HMAC-SHA256 and PBKDF2-HMAC-LSH256 in CPU Environments,” in *Information Security Applications* , Springer, Cham, 2020, pp. 321-333.