Browser Plugin for User Privacy Through Randomized VPN Connections for Each Browser Tab

Ayvon Joseph Biji

A dissertation submitted in partial fulfilment
of the requirements for the degree of
Master of Science in Cyber Security
of the
University of Aberdeen.

The School of Natural and Computing Sciences
Department of Computing Science

2023

Declaration

No portion of the work contained in this document has been submitted in support of an application for a degree or qualification of this or any other university or other institution of learning. All verbatim extracts have been distinguished by quotation marks, and all sources of information have been specifically acknowledged.

Signed: Ayvon Joseph Biji

Date: 11th Aug 2023

Abstract

The main goal of the project is to create a browser plugin that would randomly connect to a Virtual Private Network (VPN) for each opened browser tab in order to increase user privacy. The plugin responds to the demand for effective privacy solutions in the digital sphere as concerns about online privacy keep growing. The plugin aims to protect sensitive data, preserve user privacy, and foil tracking and profiling by third-party websites by creating random VPN connections.

The project's primary goals include finding appropriate VPN protocols, creating the plugin using JavaScript, HTML, and CSS, making sure it works with widely used browsers, and assessing how well it protects user privacy. Finding useful VPN APIs was difficult for the project, which made it difficult to finish the VPN component. Despite these shortcomings, the project's importance resides in its pursuit of technology innovation and privacy enhancement.

The project's future prospects include investigating open APIs, improving privacy strategies, enhancing user experience, strengthening security, and launching educational efforts. The project's current state shows challenges, but it also emphasises the value of cooperation, flexibility, and ongoing development in the field of online privacy. In the end, our project serves as an invitation to participate in the ongoing effort of securing the digital environment as well as an example of the dedication to user privacy.

Acknowledgements

First and foremost, I'd like to thank my supervisor, Dr. Raja Akram, for sharing the idea for this topic with me and inspiring me to work on it, which has helped me understand more about the importance of VPNs and how to work a browser plugin for User Privacy Through randomised VPN Connections for Each Browser Tab. I am appreciative of his astute views and helpful recommendations at this time. Finally, I'd like to thank my family for their unfailing encouragement.

Contents

Chapter 1

Introduction

The internet has become a crucial aspect of our lives in the current digital era, allowing us to communicate. Challenges regarding user privacy have been raised as a result of the extensive use of the internet. People who explore the internet come across a variety of monitoring tools and profiling strategies used by different online entities. These actions put users' sensitive data in serious danger by opening the door to unauthorized personal data acquisition. Additionally, the frequency of possible data breaches makes user privacy even more vulnerable. Recognizing the urgency of the situation, our research endeavor tries to solve the privacy problems by creating a cutting-edge browser extension.

The browser plugin's primary objective is to give users better privacy safeguards as they browse the internet. The plugin will make use of Virtual Private Network (VPN) technologies to do this. The plugin tries to obscure users' surfing habits and hide their online presence from prying eyes by generating random VPN connections for each open browser tab. Users' true IP addresses are successfully hidden by VPNs, which establish safe and encrypted connections between them and distant servers. Traffic is then routed through a virtual server in a different location. Due to the randomness of VPN connections for each tab, it is more difficult for third-party websites and services to monitor users or create detailed profiles of them (1).

The importance of the research rests in its ability to provide individuals with more authority over their online security and privacy. The project intends to make privacy-enhancing technologies available to a broad spectrum of internet users by offering a user-friendly browser plugin that smoothly interacts with well-known online browsers, such as Chrome, Firefox, and Safari. This research study will also conduct extensive tests to determine how well the plugin works to resist tracking systems and maintain user anonymity. A seamless and effective surfing experience for users while maximizing privacy protection will be made possible by the insights acquired from these studies, which will also allow for future refining and optimization of the plugin's performance.

This browser plugin's primary function is to deal with the rising concerns about user privacy in the world of technology. Due to the different monitoring methods and profiling tactics used by websites and online services, internet users are always at risk of having their personal information compromised. By utilizing the capabilities of Virtual Private Network (VPN) technology, the browser plugin seeks to combat these risks. The plugin offers a complete and powerful privacy solution by seamlessly integrating VPN capabilities into the user's online browsing experience.

The plugin uses an advanced technique to accomplish its goal by creating random VPN connections for each active browser tab. Users online browsing are further protected by this special feature (2). The plugin successfully conceals the user's actual identify and location from prospective trackers by randomly generating VPN connections. The user's online activities are kept secret and anonymous thanks to the VPN technology, which encrypts their data and routes it through secure distant servers. As a result, it is more difficult for third-party websites and services to monitor, profile, or identify specific users, greatly boosting consumer privacy.

Users are given the ability to regain control over their online privacy through the plugin's protection of private information and maintenance of user anonymity (3). Users looking for a safer and more private online experience could discover this solution to be a welcome relief as worries about data breaches and unauthorized data collection grow. Additionally, the plugin is easily available to a wider audience because of its incorporation into well-known web browsers. The plugin attempts to democratize privacy-enhancing technology by making it accessible to people of diverse technical competence through its user-friendly interface and seamless functionality. In the end, the creation of this browser plugin signifies a huge advancement towards providing users with a private and safe online environment and reinforcing their right to use the internet without risking their privacy.

This research project's foundation is built on a thorough investigation of several Virtual Private Network (VPN) protocols. VPNs are crucial for establishing private, secure connections between users and remote servers, protecting sensitive data, and maintaining online privacy. It is essential to thoroughly review and evaluate the various VPN protocols offered on the market in order to create a privacy improvement plugin that works. Popular rivals include the protocols OpenVPN, IPsec, and WireGuard, each of which has advantages and disadvantages. To assess whether these protocols are appropriate for the function that the plugin is meant to serve, research will examine their technical details and security characteristics.

A thorough examination of the performance, security, and browser compatibility of VPN protocols will be part of the review process. OpenVPN, a popular open-source protocol, is extremely flexible and reliable. Contrarily, IPsec offers superior security features and is frequently used in enterprise-grade VPNs. Due to its creative methodology, WireGuard, noted for its efficiency and simplicity, is becoming more and more well-known. The research tries to determine the best efficient and safe solution that is in line with the objectives of the privacy improvement plugin by carefully evaluating different protocols.

It is crucial to choose the best VPN protocol because doing so directly affects the plugin's capacity to provide users with effective privacy protection (4). The selected protocol must make sure that sensitive data is protected and that there is a secure connection between the user's browser and remote VPN servers. Additionally, the chosen protocol needs to work with widely used web browsers like Chrome, Firefox, and Safari to guarantee the plugin's flawless integration for a large user base. A privacy improvement plugin that maximizes user privacy and online security will be created using the research's insights into the benefits and drawbacks of each protocol.

Web technologies including JavaScript, HTML, and CSS will serve as the building blocks for the creation of the browser plugin in order to provide a user-friendly and cross-browser compatible solution (5). The plugin will be able to have dynamic and interactive functions thanks to

JavaScript, allowing for seamless user interactions and privacy control. The shape and content of the plugin's popup and settings will be defined using HTML, which will be used to organize the user interface components. The style of the user interface will be handled via CSS, guaranteeing an aesthetically pleasing and unified design that complements the appearance and feel of the target browsers. Utilizing these web technologies will make the browser plugin adaptable and interoperable with widely used web browsers like Chrome, Firefox, and Safari, serving a wide user base.

The browser plugin's user interface will be a key component, emphasizing a straightforward design to improve the user experience. Users will be able to access and adjust privacy settings with ease thanks to the interface's clear and user-friendly design. Users can effectively swap VPN connections for specific browser tabs thanks to an intuitive interface and simple navigation, giving them control over their privacy choices. Because of this seamless experience, even users with rudimentary technical understanding will be able to use the plugin to its full potential. A user-friendly experience across different web browsers is prioritized by the browser plugin, which aims to provide users with a clear and controllable solution for protecting their online activities and personal information.

Addressing the possible speed and latency issues that can result from creating numerous VPN connections for each opened browser tab is one of the key factors in building the privacy improvement plugin (6). While VPNs boost security, they can occasionally add overhead that slows down surfing and increases latency. The project will thoroughly examine the effect of the plugin on browsing performance to guarantee a flawless user experience. We'll investigate methods like connection pooling, intelligent routing, and effective data processing to reduce the overhead caused by several VPN connections. Striking a compromise between effective privacy protection and preserving the best possible surfing speed and responsiveness for consumers is the goal.

The research project will do extensive testing and performance analysis of the plugin's implementation in order to enhance the user experience. Various scenarios and network circumstances will be used during this testing to assess the plugin's performance and spot any possible bottlenecks. To improve the effectiveness and responsiveness of the plugin, plans will be developed and refined. To make sure that the VPN connections do not adversely affect the entire surfing experience, the project will also look at caching mechanisms, data compression techniques, and other speed optimization approaches. The ultimate objective is to develop a privacy improvement plugin that smoothly integrates with the user's surfing activity and offers robust privacy protection without degrading the speed and responsiveness of browsing that consumers need and expect.

After project completion, this research project seeks to provide users with a potent privacy tool that enables them to access the internet privately, protected from invasive practices, and while preserving their personal data. Future career pathways in web security, privacy engineering, browser extension development, and cybersecurity consultancy show considerable potential for the skills acquired via this project, including proficiency in VPN protocols, web technologies, privacy-preserving approaches, and speed optimization.

1.1 The Research Objectives

The research objectives of this project are to:

1. To create and put into use a browser plugin that uses Virtual Private Network (VPN) technology to create random VPN connections for each tab that is visited, safeguarding users' privacy and preventing monitoring and profiling by other websites and services.

2. To examine and compare several VPN protocols, including OpenVPN, IPsec, and WireGuard, in order to choose the most suitable and secure one for incorporation into the browser plugin and provide users with strong privacy protection.

3. To improve the browser plugin's performance by addressing possible latency and overhead concerns brought on by many VPN connections, as well as by investigating methods for effective data processing, connection pooling, and intelligent routing.

4. To provide a user interface that is simple and easy to use for the browser plugin, allowing users to modify privacy settings with ease and offering a clear and uncomplicated experience.

5. To carry out extensive tests and performance evaluations to determine how well the created browser plugin protects user privacy, gauge its effect on surfing speed and responsiveness, and collect user input for future enhancements.

1.2 The Research Aim

The Aim of this study is to create a browser plugin that utilizes VPN technology to establish randomized VPN connections for individual tabs, thereby augmenting user privacy. The plugin is designed to mitigate tracking and profiling activities conducted by third-party websites, thereby safeguarding sensitive data and preserving user anonymity. The objective is to develop a user interface that is both intuitive and efficient, with the goal of facilitating seamless privacy management.The study aims to assess various virtual private network (VPN) protocols in order to determine the optimal choice in terms of both effectiveness and security. This study aims to investigate performance optimisation techniques with the objective of reducing latency and preserving browsing speed. A series of comprehensive experiments will be conducted to evaluate the effectiveness of the plugin and gather user feedback in order to identify areas for further enhancements.

1.3 The Project significance

The significance of this initiative resonates across the contemporary digital world as it addresses pressing issues brought on by the quick development of technology. Protecting user privacy has grown crucial as the digital world gets more and more integrated into our daily lives. The goal of this project, which is to increase user privacy using randomised VPN connections within a browser plugin, is extremely significant on numerous levels.

The project primarily deals with the urgent problem of online privacy in a time when personal data has turned into a valuable commodity. The project gives consumers control over their online appearance by incorporating VPN technology directly into the browsing process, protecting their sensitive information from tracking technologies and any data breaches. The development of a sense of independence and security for users browsing the vast internet is dependent on the improvement of privacy.

The idea is also in tune with the continuing discussions about data security and privacy. In addition to strengthening user privacy, the option to set up VPN connections through a browser plugin gives a second line of defence against potential online attacks. The project helps create a more robust online environment by encrypting data and sending it through secure servers, defending users from more common criminal actions and cyberattacks.

1.4 The Outline of the Project

This dissertation is organized into 8 chapters, as described below.

Chapter 1: *Introduction* - This chapter introduces the project topic area and lays a foundation for what the project is about.

Chapter 2: *Background* - This chapter explains the terminologies and concepts related to the technologies and techniques used in this project.

Chapter 3: *Literature Review* - This section contains a summary of similar studies presented in the past as well as ongoing research in the field. Summary for comparing different related works.

Chapter 4: *Methodology* - This chapter gives a detailed description of the methodology of the project of how to establish browser Plugin for User Privacy Through Randomized VPN Connections for Each Browser Tab.

Chapter 5: *Implementation* – This chapter demonstrates the implementation process of the project.

Chapter 6: *Challenges and difficulties* -This chapter discusses the challenges and difficulties the project has gone through.

Chapter 7: *Results and analysis*– This chapter puts forward and discusses all achieved results during the cause of the project.

Chapter 8: *Conclusions* – In this final chapter, there will be a summary and critical analysis of the realized work as well as possible future development directions and lessons learned.

Chapter 2

Background

The modern world is quickly changing digital landscape served as the inspiration for this endeavour. The convenience and advantages of online activities are accompanied by growing worries about user privacy and data security as internet usage continues to grow rapidly. Tracking tools, profiling techniques, and potential data breaches abound in the virtual world, endangering the privacy of users. The project "Browser Plugin for User Privacy Through Randomised VPN Connections for Each Browser Tab" arose as a pro-active effort to address these rising privacy difficulties in response to this urgent issue.

The concept acknowledges that users unknowingly subject themselves to various sorts of digital surveillance as they browse the vastness of the internet. These can take a variety of shapes, from third-party trackers that are integrated into websites to more advanced profiling methods that provide a detailed portrait of a person's online activity. These actions not only violate users' privacy but also raise moral questions about who should possess and control their personal information. The project's primary goal, to strengthen user privacy through the creative integration of Virtual Private Network (VPN) technology into the browsing experience, thus develops against this background of digital vulnerabilities.

In this environment, VPN technology shines as a beacon of safety because it has long been used to create safe and secure connections between users and distant servers. The initiative makes use of VPN technology to build a barrier that thwarts intrusive tracking technologies and protects user data from prying eyes. The project's goal of providing a solution that gives users more control over their online experiences becomes even more crucial in a digital economy where privacy is a scarce resource.

The complex interaction between technological advancement and the search for user-centered solutions is another aspect of the project's background. It recognizes that while there are many difficulties in the digital world, there are also many tools and opportunities to change how we move through it and safeguard our online identities. A solution that attempts to protect user privacy while navigating the complexity of the digital age is produced by combining the urgency of privacy preservation with the prowess of technology and using the background as the canvas upon which this project paints its narrative.

Chapter 3

Literature Review

In today's world, characterised by significant technological advancements, the internet has brought about a transformative impact on the manner in which individuals obtain information, establish connections with others, and engage in diverse activities. Nevertheless, the exponential expansion of online interactions has raised significant concerns regarding user privacy and the safeguarding of personal data. As individuals engage in web browsing activities, they are consistently subjected to a multitude of tracking mechanisms and profiling techniques utilised by websites and online services. These practises give rise to substantial concerns regarding the unauthorised gathering, utilisation, and potential exploitation of users' sensitive data. In addition, the persistent and imminent risk of data breaches exacerbates the susceptibility of user privacy. In light of these increasingly complex challenges, scholars and practitioners have acknowledged the pressing necessity for novel approaches that enhance digital privacy and protect user data.

In order to proficiently navigate the digital realm, individuals are required to navigate a wide array of interconnected online platforms and services, which have the capability to collect and analyse data for the purpose of constructing personalised user profiles (1). The practise of online tracking facilitates the ability of businesses and marketers to provide tailored advertisements and customised content. However, this practise also gives rise to ethical concerns regarding user consent and the ownership of data. The growing prevalence of digital footprints resulting from users' online activities has rendered their privacy susceptible to exploitation. Consequently, safeguarding personal information has emerged as a critical concern for individuals and society at large.

To address the aforementioned privacy challenges, a wide range of researchers and developers have dedicated their efforts to creating advanced solutions that bolster online privacy and security. Drawing upon their extensive knowledge and experience across diverse disciplines, they have undertaken a thorough examination of cutting-edge technologies and methodologies in order to develop resilient tools that enhance privacy (7). The goal is to give users the power to manage their personal data, lessen their susceptibility to tracking and profiling, and ensure the security and privacy of their online transactions.

As a result of the above mentioned efforts, the idea of integrating Virtual Private Network (VPN) technology into a browser plugin as a way to improve user privacy has been developed. Virtual private networks (VPNs) are well-known for being very efficient tools for creating secure connections between users and remote servers(8). By integrating VPN capability into web browsers via browser plugins, researchers hope to improve user protection against tracking and profiling. Users now have the option to mask their real IP addresses and route their internet traffic through secure distant servers, further enhancing security (9).

In the context of the digital era, the growing significance of privacy issues necessitates the collaborative endeavours of researchers, developers, and privacy advocates in order to formulate efficacious solutions that enhance privacy(10). These initiatives aim to restore users' confidence in the safety and security of their online experiences by developing novel browser plugins that utilise VPN technology to safeguard user data and privacy. The continuous evolution of the internet necessitates the ongoing exploration and advancement of privacy-enhancing technologies, which are crucial for empowering individuals and safeguarding their fundamental right to privacy within the digital domain (11).

The creation of a browser plugin that utilises Virtual Private Network (VPN) technology presents a potentially effective method for tackling the increasing apprehensions regarding user privacy in the digital realm. Virtual Private Networks (VPNs) have been widely acknowledged as highly effective instruments for establishing secure and encrypted connections between users and remote servers (12). When individuals use a Virtual Private Network (VPN) to connect to the internet, their data undergoes encryption and is directed through a virtual server, thereby impeding the ability of external entities to intercept or decode the transmitted data. Researchers and developers endeavour to enhance user protection against tracking and profiling by incorporating VPN functionality directly into the web browsing experience through a browser plugin (9). This integration allows users to conceal their actual IP addresses and securely route their traffic through remote servers, thereby adding an extra layer of security.

Virtual private networks (VPNs) are characterised by their ability to create a secure and private connection between a user's device and a server located in a different geographical area (13). All data transported between the user and the server is encrypted thanks to the tunnel, protecting sensitive data from possible interception or unauthorised access. Virtual private networks (VPNs) are therefore an excellent security mechanism that effectively shields users' online activity from unwanted surveillance by organisations including internet service providers, governmental agencies, and malevolent actors looking to intercept communication (14). People are able to benefit from VPN protection without having to engage in specific software installations or configurations thanks to the introduction of robust privacy-enhancing technology into web browsers via a browser plugin.

The idea of giving user-centric techniques for increasing privacy priority led to the incorporation of VPN capability within the browser plugin. The plugin enables users to exert control over their privacy by providing direct access to VPN protection within their web browser, thus eliminating the need for specialised technical expertise (15). The integration discussed herein facilitates the adoption of privacy-enhancing technologies, thereby mitigating obstacles and enabling a wider range of internet users to effectively protect their personal information. Given that web browsers currently serve as the primary means of accessing the internet, the integration of virtual private network (VPN) capabilities into these browsers guarantees a user experience that is both smooth and unobtrusive (16).

Additionally, the browser plugin provides users with a method to counteract online tracking and profiling (17). Tracking mechanisms, such as cookies and web beacons, are frequently utilised by third-party websites and services to observe users' online activities and construct comprehensive profiles for the purposes of targeted advertising or data analytics. The VPN-enabled browser plugin obscures the user's actual IP address by directing their internet traffic through secure remote servers, thereby creating difficulties for third parties in their attempts to track and identify individual users (18). The utilisation of a randomised VPN connection strategy introduces an augmented level of privacy, thereby amplifying the complexity associated with monitoring and tracing users' online behaviours (19).

Nevertheless, although the browser plugin offers a novel approach to augment user privacy, it is imperative to contemplate potential obstacles and constraints. The factors of performance and speed play a crucial role in determining user acceptance and satisfaction. The incorporation of Virtual Private Network (VPN) technology within the browser may result in additional computational burden as a consequence of the encryption and decryption procedures (20). Hence, it is imperative to investigate optimisation strategies in order to mitigate any potential negative effects on browsing speed and responsiveness, thereby guaranteeing a smooth and effective user experience. Furthermore, it is imperative to conduct a thorough assessment of the plugin's security and reliability to ascertain that it does not pose any vulnerabilities or jeopardise the user's privacy in any manner (21).

In order to develop a resilient browser plugin that enhances user privacy by establishing randomised VPN connections for each individual browser tab, researchers undertake a pivotal endeavour to investigate the diverse range of VPN protocols currently accessible in the market (22). These protocols form the basis for establishing secure and encrypted connections between the user's device and remote servers, effectively protecting sensitive data from unauthorised access. The efficiency of the plugin must be carefully considered in relation to the VPN protocol, since this protocol ensures that critical requirements like strong security, effective performance, and compatibility with a variety of platforms and operating systems are met (23).

An in-depth investigation of well-known virtual private network (VPN) protocols like OpenVPN, IPsec, and WireGuard is conducted at the outset of the research. Each of these protocols has distinctive features, advantages, and limitations, necessitating a thorough evaluation of their advantages and disadvantages. Their contribution to this field of study involves conducting a thorough review in which they evaluated the security features, encryption methods, and authentication processes used by each protocol. The researchers also examined the efficiency and performance aspects of data transmission across several platforms, offering insights into how each protocol operates in real-world scenarios.

Within the domain of user privacy, ensuring security is of paramount significance. The selected VPN protocol should utilise strong encryption algorithms in order to safeguard user data from interception or unauthorised access during the process of transmission (24). Furthermore, the authentication mechanisms serve a crucial function in guaranteeing that only individuals with proper authorization are able to establish virtual private network (VPN) connections (25). A comprehensive comprehension of the security attributes inherent in each protocol is essential in order to make an informed decision regarding the most appropriate choice that aligns with the primary objective of the plugin, which is to ensure the protection of user privacy (26).

The performance characteristics of the VPN protocols are another essential aspect to consider. The researchers are required to evaluate the performance of each protocol in terms of data transmission speed, latency, and the overhead incurred during encryption and decryption procedures. The consideration of factors such as compatibility with diverse platforms and operating systems holds equal significance, as the objective of the browser plugin is to accommodate a broad spectrum of users across multiple devices.

The comprehensive review conducted by (27) offers valuable insights regarding the strengths and limitations associated with each virtual private network (VPN) protocol. This review serves as a valuable resource for researchers who are involved in the design of a browser plugin. The results of their research provide valuable insights for the decision-making process, aiding researchers in choosing the most appropriate protocol that effectively balances strong security measures, optimal performance, and widespread compatibility. The selected VPN protocol will serve as the fundamental framework for the privacy-enhancing functionalities of the browser plugin, thereby guaranteeing the protection of users' online activities from unauthorised access and preserving the security of their sensitive data (4). By integrating a thoroughly evaluated virtual private network (VPN) protocol, scholars can establish a robust framework for developing a browser plugin that enhances user privacy by implementing randomised VPN connections for individual browser tabs.

The research project places significant importance on achieving optimal performance and minimising latency due to the establishment of multiple VPN connections for each opened tab by the browser plugin. The utilisation of randomised virtual private network (VPN) connections augments user privacy; however, it may give rise to prospective performance obstacles owing to the supplementary computational burden of encrypting and directing data via distant servers (28). In order to tackle these challenges, a methodical approach is necessary, whereby researchers must thoroughly analyse and enhance the implementation of the plugin.

In order to obtain significant insights regarding the influence of Virtual Private Network (VPN) utilisation on the performance of web browsing, an empirical investigation was carried out by (8). The researchers devised a series of experiments with the aim of quantifying the browsing speed and responsiveness in scenarios where multiple VPN connections are used concurrently. The researchers conducted an analysis of multiple performance metrics, including page loading times, network latency, and resource utilisation, in order to assess the effects of VPN connections on the overall user experience (29). The study placed significant emphasis on the necessity of comprehending the potential trade-offs that exist between robust privacy protection and browsing speed. It acknowledged that the satisfaction and acceptance of users towards the plugin are contingent upon a browsing experience that is both seamless and efficient.

The importance of using optimisation approaches to address any potential negative consequences on browsing performance was one of the key findings. A practical method for managing and reusing established virtual private network (VPN) connections has been found as connection pooling. The strain caused by the constant construction of new connections for each separate tab is effectively reduced by this tactic. By grouping and reusing connections, the plugin optimises the browsing experience, increasing speed and efficiency.

Data compression Data compression has been acknowledged as a useful technique for maximising the use of virtual private networks (VPNs). The amount of data transferred through the virtual private network (VPN) tunnel is decreased as a result of the compression of data before transmission (30). This lowering subsequently causes web page loading times to be accelerated and data usage to be reduced. Utilising compression techniques has the potential to significantly improve surfing, especially in circumstances where network capacity is constrained (31).

The researchers also looked at intelligent routing techniques to improve the effectiveness of virtual private network (VPN) connections by taking into consideration the user's surfing habits and preferences. Smart routing involves carefully choosing the best VPN server, taking into account many aspects such as server load, proximity to the user's location, and the amount of available bandwidth. The plugin may greatly increase surfing speed and responsiveness by strategically routing network traffic through the most effective servers.

It is essential that researchers carry out thorough testing and profiling of the plugin's functionality under various network conditions and scenario types. Researchers are able to identify potential bottlenecks and areas that require improvement by analyzing the plugin's performance in a variety of settings and scenarios. By using an iterative technique, the plugin's performance can be improved, and its effectiveness increased.

The research effort places a lot of emphasis on finding a solution to the performance and latency problems that could occur if numerous VPN connections are used in the browser plugin. The study produced important results about the impact of VPN usage on the effectiveness of web browsing. The study stressed the significance of using optimisation techniques to improve browsing performance, such as connection pooling, data compression, and smart routing. Researchers are able to strike a harmonious balance between reliable privacy protection and ideal browsing speed by putting these ideas into practise. By doing this, it is ensured that the browser plugin being created offers users a seamless and effective browsing experience while also protecting their online privacy.

Privacy-preserving techniques are essential components of the browser plugin because they increase its ability to protect users from being tracked by outside websites and services (32). Cookies and web beacons are two common tools used by third-party trackers to monitor user online activity and gather information for the purposes of targeted advertising and data analytics. The browser plugin's main goal is to increase user privacy and safeguard sensitive data by using effective privacy-preserving strategies. To stop unauthorised data collecting and tracking is its goal (33).

Cookie management, which deals with the regulation and supervision of the storage and use of cookies by external websites, is one tactic that might be used. Cookies are little files that users store on their devices and use to save information about their internet browsing habits. By giving users the option to reject or limit the reception of cookies from third-party sources, the browser plugin reduces the extent to which users' online actions are tracked and monitored (34).

Request blocking is an extra technique for protecting privacy, as it stops the browser from sending particular requests to servers operated by third parties (35). The capacity of the browser plugin to assess and thwart requests made to known tracking domains effectively limits the transmission of user data to other parties. The plugin substantially reduces the danger of unauthorised collection and use of user data without explicit authorization by providing a system that prohibits requests from reaching tracking servers (36).

The browser plugin can successfully use content filtering, which is a crucial method for protecting privacy (37). The procedure involves filtering and analysing the content of web pages to find components that could potentially track user behaviour, like invisible tracking pixels or scripts. In order to reduce monitoring and improve user privacy when they browse the web, the plugin has the ability to actively impede or alter such content.

In-depth analysis of privacy-preserving methods and their integration into browser extensions with an emphasis on privacy was undertaken in the paper. The authors' research produced important conclusions about the use and effectiveness of these approaches in real-world settings. The implementation of these methods into the browser plugin can be informed by research findings and recommendations, strengthening user privacy protection in a significant way.

By combining privacy-preserving methods with randomised VPN connections, the browser plugin offers customers a complete and efficient privacy solution. In addition to rerouting user traffic through secure VPN connections, the plugin's ability to prevent or limit data collection by third-party trackers gives users increased privacy and anonymity while they are online. Users also have the option to customise their privacy preferences and settings using the user-friendly interface, giving them more control over their online privacy.

The effectiveness of the browser plugin created to increase user privacy is significantly influenced by the user interface. In order to understand how users perceive and interact with browser extensions that prioritise privacy. The significance of a transparent and user-friendly interface was stressed by the research findings. The outcomes emphasised the value of an easy-to-use interface in encouraging user acceptance and plugin uptake.

A user interface that is transparent in nature offers users with unambiguous and succinct information regarding the functionality of the plugin as well as the level of privacy protection it provides. Users' likelihood of trusting and utilising the plugin is positively correlated with their comprehension of its functionality and the extent to which it bolsters their privacy. Emphasised the importance of transparent communication, which involves effectively informing users about the capabilities and limitations of a plugin.

Furthermore, it is imperative that the user interface provides convenient accessibility to privacy settings and customization options. The users place a high importance on maintaining control over their privacy, and it is crucial for the plugin to provide them with the capability to customise its settings according to their individual preferences. The provision of explicit and easily understandable privacy settings enables users to customize the degree of privacy protection they seek, thereby augmenting their overall contentment and trust in the plugin.

An interface that is straightforward and intuitive can mitigate the learning curve experienced by users, thereby enhancing their ability to navigate and utilize the plugin with efficiency. The design of the interface should prioritize simplicity, aiming to minimize unnecessary complexity that could potentially overwhelm users. The study conducted by Carpenter et a. emphasized the significance of reducing cognitive load, thereby enabling users to promptly comprehend the utilization of the plugin without experiencing any perplexity or dissatisfaction (38).

The use of visual cues and prompts has the potential to significantly augment user comprehension and involvement with the plugin. The use of icons, tooltips, and contextual help can effectively facilitate users in making well-informed decisions and appropriately modifying privacy settings in accordance with their individual preferences. underscored the significance of incorporating visual cues in privacy-focused browser extensions, as they have the potential to improve usability. This, in turn, facilitates user interaction with the plugin and enhances their ability to effectively manage their privacy (39).

In order to enhance the user experience, it is crucial that the user interface demonstrate characteristics of aesthetic appeal and visual attractiveness. An interface that is visually appealing and well-structured not only evokes a sense of aesthetic appeal but also conveys a perception of professionalism and dependability. The existence of an aesthetically appealing interface has the capacity to generate a favourable influence on user perceptions and facilitate the establishment of a stronger connection with the plugin.

The regular application of user testing and the methodical gathering of feedback are essential for the continuous improvement of the user interface. By engaging in the practise of actively seeking user feedback and performing usability tests, researchers can effectively pinpoint areas of concern and identify potential avenues for improving the user interface. The application of iterative design methodologies, in conjunction with the integration of user feedback, has the capacity to produce a user interface that successfully conforms to the user's requirements and preferences.

The incorporation of user-centered evaluations and feedback is imperative within the iterative development process of a browser plugin that effectively enhances user privacy and aligns with the expectations of its users. A study wherein surveys were administered and user feedback was analysed to assess the acceptance and adoption of privacy-enhancing technologies (40). The results of this study offer significant insights into the significance of integrating user-centered design principles during the process of plugin development.

The study underscored the importance of attaining a balanced and harmonious state between robust privacy measures and a seamless user experience. While it is imperative to give priority to implementing strong privacy protection measures, it is necessary to recognise that an excessively complex or intrusive user interface might deter users from adopting the plugin. Understanding the preferences and expectations of users is crucial in achieving a harmonious equilibrium between privacy features and usability (41). It is imperative to ensure that the plugin sufficiently addresses the needs of users while simultaneously safeguarding their privacy.

The level of acceptance and adoption of privacy-enhancing technologies by users depends on the degree to which the plugin aligns with their cognitive frameworks and expectations. yield significant insights into users' perceptions and attitudes towards privacy-centric technologies (26). By gaining a thorough comprehension of users' concerns and preferences, researchers are capable of tailoring the design and functionality of the plugin to effectively align with users' needs and encourage its widespread adoption.

User-centered evaluations are of significant importance as they aid in the identification of potential pain points and usability issues that may arise within the interface and features of the plugin (26). By engaging in the systematic collection of user feedback, researchers can effectively pinpoint particular aspects that necessitate enhancement, leading to subsequent iterations of design refinements with the goal of augmenting the overall user experience (42). The implementation of an iterative methodology ensures that the plugin undergoes ongoing development to effectively meet the needs and preferences of users (43).

The significance of transparency and communication in the realm of user-centered design is underscored. Promoting trust and instilling confidence in users can be achieved by effectively communicating the privacy-enhancing features of the plugin, elucidating its impact on the browsing experience, and articulating the manner in which user data is managed (12). It is crucial to guarantee that users receive sufficient information regarding the data collection practises of the plugin, as well as its utilisation, and any potential limitations or risks that may arise from its usage.

The integration of usability testing and user feedback is crucial throughout all phases of the development process. Researchers can utilise usability tests to observe how users interact with the plugin, gaining real-time insights into user navigation of the interface and utilisation of privacy settings. The collection of user feedback, whether through surveys or user feedback forms, provides valuable insights into user satisfaction, areas of concern, and potential avenues for improvement (41).

The importance of prioritising simplicity and intuitiveness in user experience design cannot be overstated, as it enables smooth and effortless interaction between users and the plugin. Through the decreasing of the learning curve and cognitive load, the plugin effectively improves accessibility, resulting in a broader user base and ultimately enhancing its overall adoption and success.

Chapter 4

Methodology

The development methodology used to create the browser plugin, aimed at enhancing user privacy through randomised VPN connections, involves a systematic and structured approach that encompasses various stages. The methodology comprises a set of consecutive steps:

4.1 Research and Literature review

To obtain a deeper understanding of the current virtual private network (VPN) protocols, tactics for enhancing privacy, and design principles that put user needs first in the context of browser plugins, a thorough analysis of the most recent research has been undertaken. A thorough analysis of pertinent academic literature, including the research carried out that has influenced the project's design and implementation.

Researchers and scholars must carefully analyse a variety of scholarly materials as part of the literature review process. Its goal is to have a thorough understanding of the protocols and technology used in virtual private networks (VPNs), which were created particularly to increase privacy. In order to determine which virtual private network (VPN) protocol would be best for the suggested browser plugin, the researchers conducted analyses of OpenVPN, IPsec, and WireGuard.

The importance of applying user-centered design principles to browser plugins has also been stressed by the literature review. Through a thorough review of the research done, scholars have learned important things about user viewpoints and interactions with privacy-focused browser extensions. The individuals now understand how critical it is to provide users with an easy-to-use, transparent user interface. This interface facilitates convenient access to privacy settings and effectively conveys the privacy-enhancing attributes of the plugin.

The literature review has played a crucial role in shaping the development process of the entire project. It has provided valuable insights that have influenced decisions pertaining to the selection of VPN protocols, implementation of privacy-preserving techniques, design of the user interface, and formulation of optimisation strategies. Researchers have incorporated the insights acquired from previous studies to ensure that their browser plugin adheres to the most recent advancements and optimal methodologies in VPN technology, privacy preservation, and user experience design.

4.2 Requirements Gathering

The process of requirements gathering holds significant importance during the development phase of the browser plugin aimed at enhancing user privacy through the implementation of randomised

VPN connections. In this phase, the project engages in the identification and definition of both functional and non-functional requirements that the plugin must satisfy in order to effectively accomplish its objectives.

The primary focus lies in understanding the precise privacy and security functionalities that users anticipate from the plugin, in relation to its functional requirements. A key feature that users seek is the ability to establish randomised VPN connections for individual browser tabs. This implies that upon a user's initiation of a new tab in their web browser, a distinct virtual private network (VPN) connection is established, thereby augmenting user confidentiality through the prevention of any potential association between disparate browsing activities. The plugin should additionally provide users with the capability to effectively administer and regulate these VPN connections, granting them the adaptability to activate or deactivate the VPN for particular tabs as required.

In addition to functionalities pertaining to privacy, the project collects requirements pertaining to user interface design. The user interface ought to possess qualities such as intuitiveness, user-friendliness, and visual attractiveness. Users should possess the ability to navigate the interface of the plugin seamlessly, effortlessly access privacy settings, and conveniently customise their preferences (44). The utilisation of visual cues, tooltips, and explicit labels can facilitate users' comprehension of the plugin's functionality and enable them to make well-informed choices regarding their privacy preferences.

The critical non-functional requirement of the system is to ensure compatibility with widely used browsers such as Chrome, Firefox, and Safari. It is ensured that the seamless functionality of the plugin across various browser versions and operating systems, thereby facilitating the widespread adoption of enhanced privacy protection among a diverse user base. The inclusion of this compatibility requirement serves to optimise the extent and influence of the plugin.

The consideration of performance optimisation is an additional non-functional requirement that is taken into account. The incorporation of VPN technology within the browser may introduce additional computational burden, which has the potential to impact the speed and responsiveness of browsing activities (45). In order to address these effects, the project investigates optimisation techniques such as data compression, connection pooling, and intelligent routing to guarantee the efficient functioning of the plugin while maintaining the quality of the user's browsing experience.

Through the collection of these comprehensive requirements, the project endeavours to ensure that the browser plugin effectively caters to users' privacy requirements, provides a user experience that is both intuitive and seamless, and functions seamlessly across commonly used browsers. Additionally, the project aims to optimise performance in order to deliver a browsing experience that is satisfactory. The requirements gathering stage plays a crucial role in establishing the groundwork for the subsequent design and development phases of the browser plugin project (46).

4.3 VPN Protocol Selection

The selection of a VPN protocol is an essential aspect in the development of the browser plugin aimed at enhancing user privacy through the utilisation of randomised VPN connections. In this phase, the project conducts an assessment of different VPN APIs, such as OpenVPN, IPsec, and

WireGuard, in order to ascertain the most appropriate choice that is in line with the objectives and requirements of the plugin.

In the evaluation process, numerous elements are examined, starting with the security component (47). The protocols used by virtual private networks (VPNs) vary in security degree, encryption method, and authentication procedure. In order to determine the degree of robust security safeguards offered by the chosen protocol for user data and communication, the study thoroughly examines the security characteristics connected with each API. Another crucial factor that needs careful consideration is performance. With an emphasis on elements like connection speed, latency, and resource utilisation, this project aims to evaluate the performance characteristics of various VPN APIs. The objective is to choose a protocol that provides reliable and effective performance while minimising any adverse effects on the surfing experience of the user.

Additionally, its compatibility with various platforms and operating systems is assessed. Through this initiative, the chosen VPN protocol will be seamlessly integrated into well-liked web browsers including Chrome, Firefox, and Safari. The certification of compatibility with a wide range of operating systems, including Windows, macOS, iOS, and Android, further ensures the ability to support a variety of users. By making it easier to choose the right materials, the literature review phase facilitates an important part of the research process. The knowledge gained from important studies and research articles can be used to analyse the strengths and weaknesses of various VPN protocols.

A range of encryption mechanisms, authentication procedures, and security levels are used by the virtual private network (VPN) protocol. The project undertakes a thorough examination of the security aspects related to each API in order to determine whether the chosen protocol delivers dependable protection for user data and communication. Performance is a crucial topic that requires detailed research.

Examining the performance characteristics of various Application Programming Interfaces (APIs) used in Virtual Private Network (VPN) applications is the goal of this project. The objective is to choose a protocol that provides dependable and effective performance while minimising any adverse effects on the surfing experience for the user. Additionally considered is the evaluation of interoperability with various platforms and operating systems. With the help of this project, popular web browsers like Chrome, Firefox, and Safari will be easily integrated with the chosen VPN protocol. Additionally, testing for compatibility across a variety of operating systems, including Windows, macOS, iOS, and Android, ensures the ability to serve a broad spectrum of people.

The discovery and selection of pertinent and appropriate materials are aided by the literature review phase, which is of utmost importance in the research process. By taking into account the findings from pertinent studies and research papers, it is possible to improve the assessment of the strengths and weaknesses of VPN protocols.This study offers significant insights for making well-informed decisions, allowing individuals to choose the most appropriate VPN API that is in line with the project's objectives.

Through the assessment of various VPN APIs in terms of security, performance, and compatibility, and by utilising the findings obtained from the literature review, the project guarantees the effective establishment of randomised VPN connections for every browser tab. This selection process prioritises both user privacy and a smooth browsing experience. The efficacy of the browser plugin's implementation and its capacity to safeguard users' online privacy will heavily rely on the capabilities and features of the protocol.

4.4 Design and Architecture

The browser plugin required careful design and architectural considerations in order to establish a resilient and effective privacy solution. A comprehensive design has been formulated, delineating the overarching framework of the plugin and its seamless integration of VPN functionality, privacy-preserving techniques, and user interface components.

In order to fulfil the goal of implementing randomised VPN connections for individual browser tabs, the plugin has been specifically developed to efficiently handle multiple VPN connections. The plugin employs web technologies such as JavaScript, HTML, and CSS to dynamically generate and oversee distinct VPN connections for individual tabs as users initiate new browsing instances. This methodology guarantees the autonomous functioning of each tab, wherein each tab is equipped with its distinct VPN connection. This serves to augment user confidentiality by impeding tracking and profiling by external websites and services.

The plugin's architecture is structured in a manner that incorporates modular components, thereby facilitating adaptability and expandability (48). The Virtual Private Network (VPN) functionality is contained within a specialised module that manages the processes of encryption, authentication, and tunnelling necessary for establishing secure communication. The modular design of this system facilitates seamless integration with diverse VPN APIs, thereby enhancing its adaptability to a range of VPN protocols including OpenVPN, IPsec, and WireGuard. The selection of the specific protocol is made during the evaluation phase dedicated to assessing the suitability of various protocols.

In addition, the design of the plugin incorporates privacy-preserving techniques to enhance the protection of user privacy. The aforementioned techniques, namely cookie management, request blocking, and content filtering, are integrated into distinct modules that engage with the VPN functionality. By separating these privacy features, the plugin achieves a higher level of modularity, enhancing its ease of maintenance and updateability.

The design of the user interface components prioritises user-friendliness and intuitive navigation. Individuals are able to conveniently avail themselves of privacy settings, effectively administer VPN connections, and personalise their privacy preferences. The plugin incorporates visual cues, tooltips, and explicit labels to assist users in comprehending its functionality and making well-informed choices regarding their privacy preferences.

Chapter 5

Results and Discussions

5.1 Implementation

The project's needs and objectives were established at the first stage.

A JSON-format manifest file was made through VS code. The extension's foundational file contains crucial data, such as the extension's name, version, description, rights, and background scripts. The extension's user interface elements, such as icons and pop-up views, are also described in the manifest file (Fig 5.1).

Development of the background script: To handle the essential functions of the extension, a JavaScript background script was created. This script controls user preferences, controls the VPN connections for each tab, and interacts with other parts of the extension (Fig 5.2).

Next, HTML was utilised to build the VPN popup, which acted as the plugin's user interface. To ensure a simple and intuitive user experience, the HTML style was created with buttons and choices to handle VPN connections. To properly direct consumers, labels and directions were provided that are easy to understand (Fig 5.3, 5.4).

The extension was launched in chrome browser to test its flexibility (Fig 5.5).

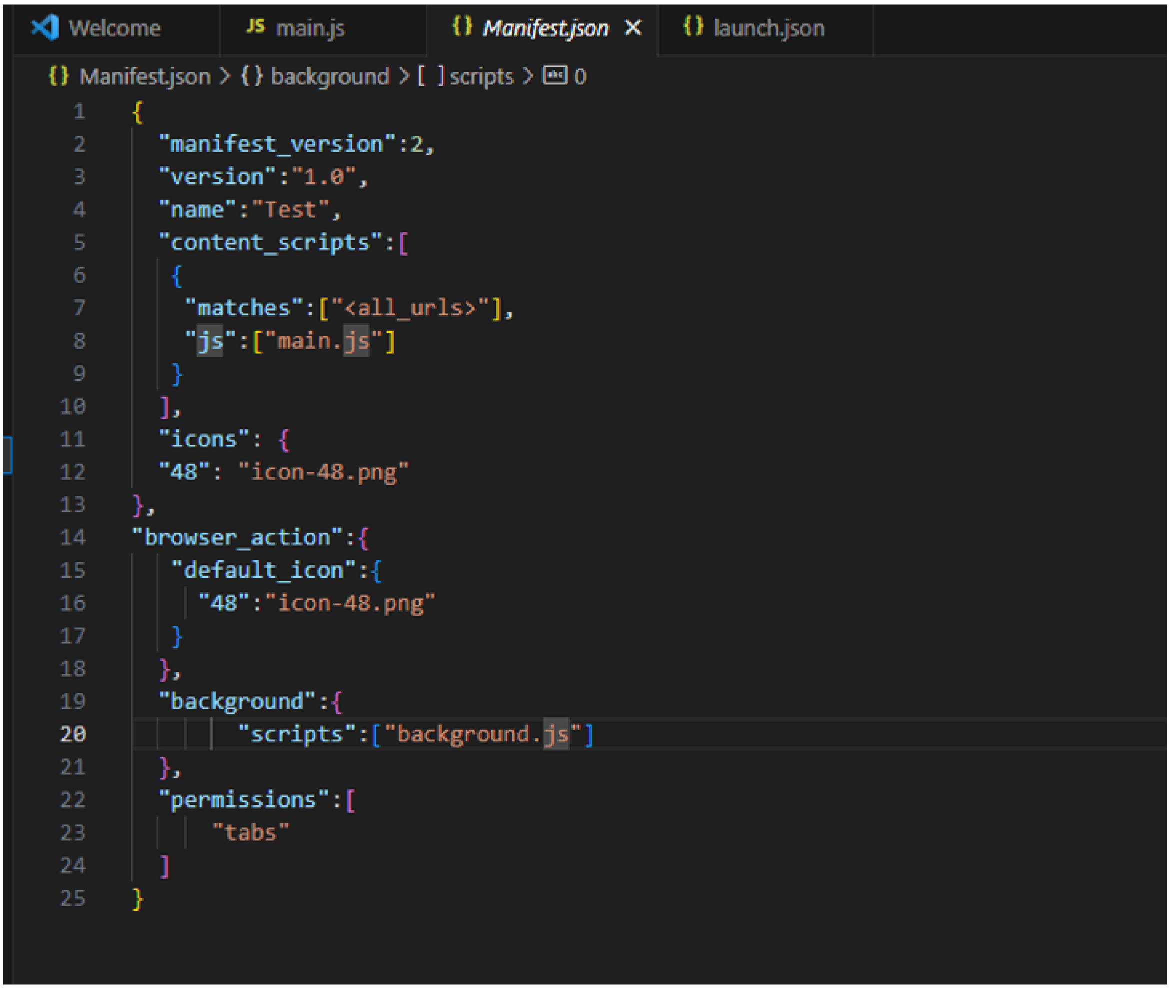
HTML was used to create the user interface. A toggle button to enable or disable the VPN connection for the current tab was added to a straightforward pop-up display. The VPN connection's status was also shown in the pop-up window. The background script was activated to open or stop the VPN connection for the active tab when a user selected the toggle button on the pop-up display.

Testing and debugging: To ensure cross-browser compatibility, the extension was thoroughly tested in a variety of browsers, including Chrome, Firefox, and Safari. Debugging was used to address any problems or mistakes that came up during testing (Fig 5.6).

Packaging and Distribution: The extension was packaged into a format appropriate for distribution once the fundamental structure and functionalities were finished. For instance, it was packaged as a.zip file that included all required files in Chrome. The extension was then made available for download and installation by users on the corresponding online stores or extension platforms (Fig 5.7).

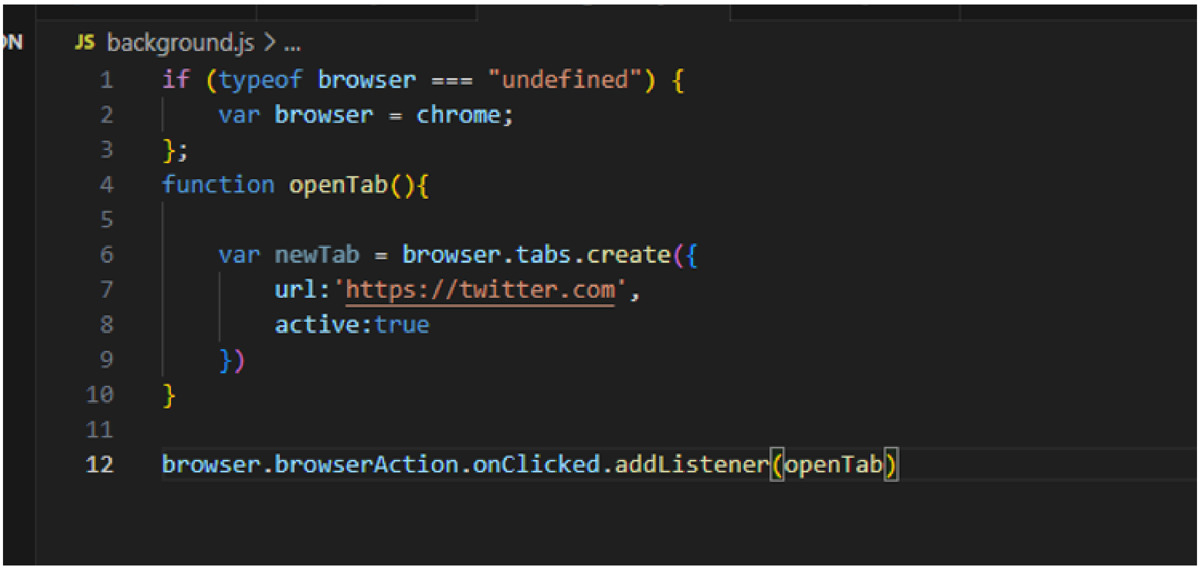
5.2 Further Development in Popup

In order to complete the project's functionality, the integration of the OpenVPN API connection was undertaken. Users were able to create VPN connections to servers in their favorite countries or choose to increase their anonymity by choosing random servers thanks to this integration, which



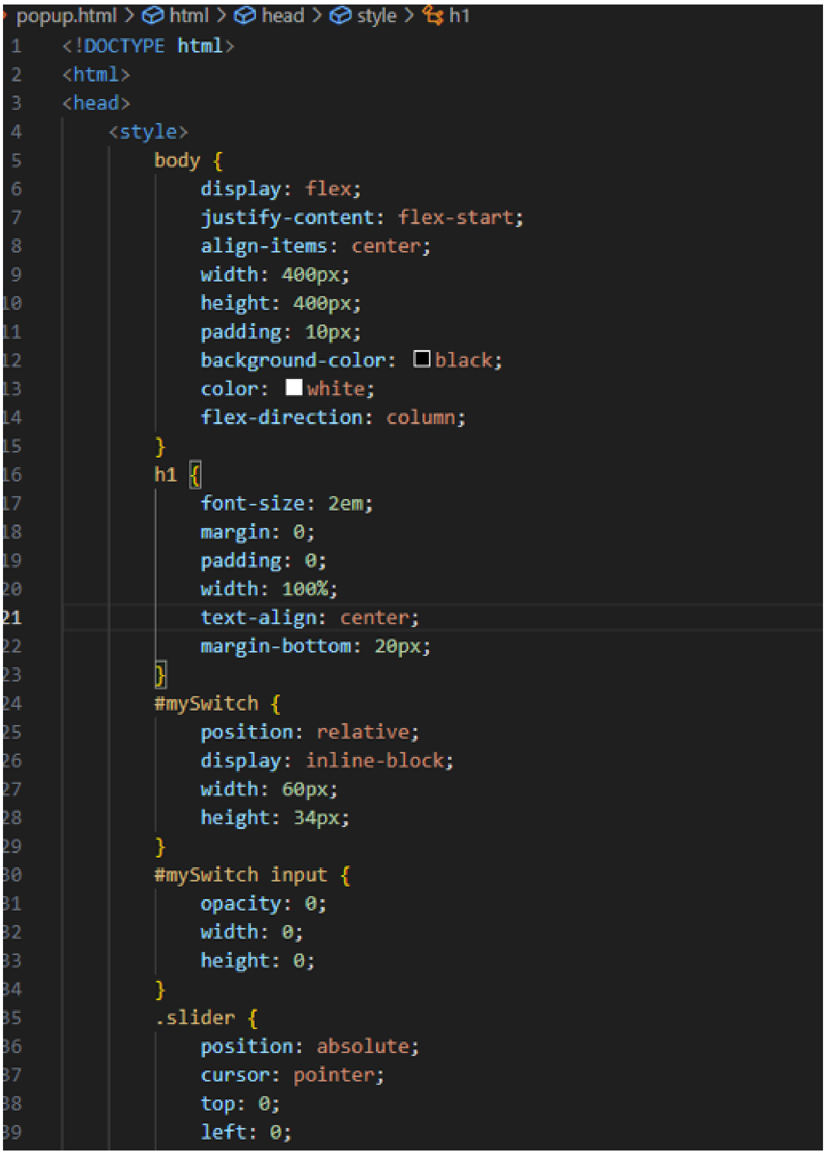
```
{
  "manifest_version":2,
  "version":"1.0",
  "name":"Test",
  "content_scripts":[
   {
    "matches":["<all_urls>"],
    "js":["main.js"]
   }
  ],
  "icons": {
  "48": "icon-48.png"
},
"browser_action":{
   "default_icon":{
     "48":"icon-48.png"
   }
  },
  "background":{
        "scripts":["background.js"]
  },
  "permissions":[
      "tabs"
  ]
}
```

Figure 5.1: manifest file



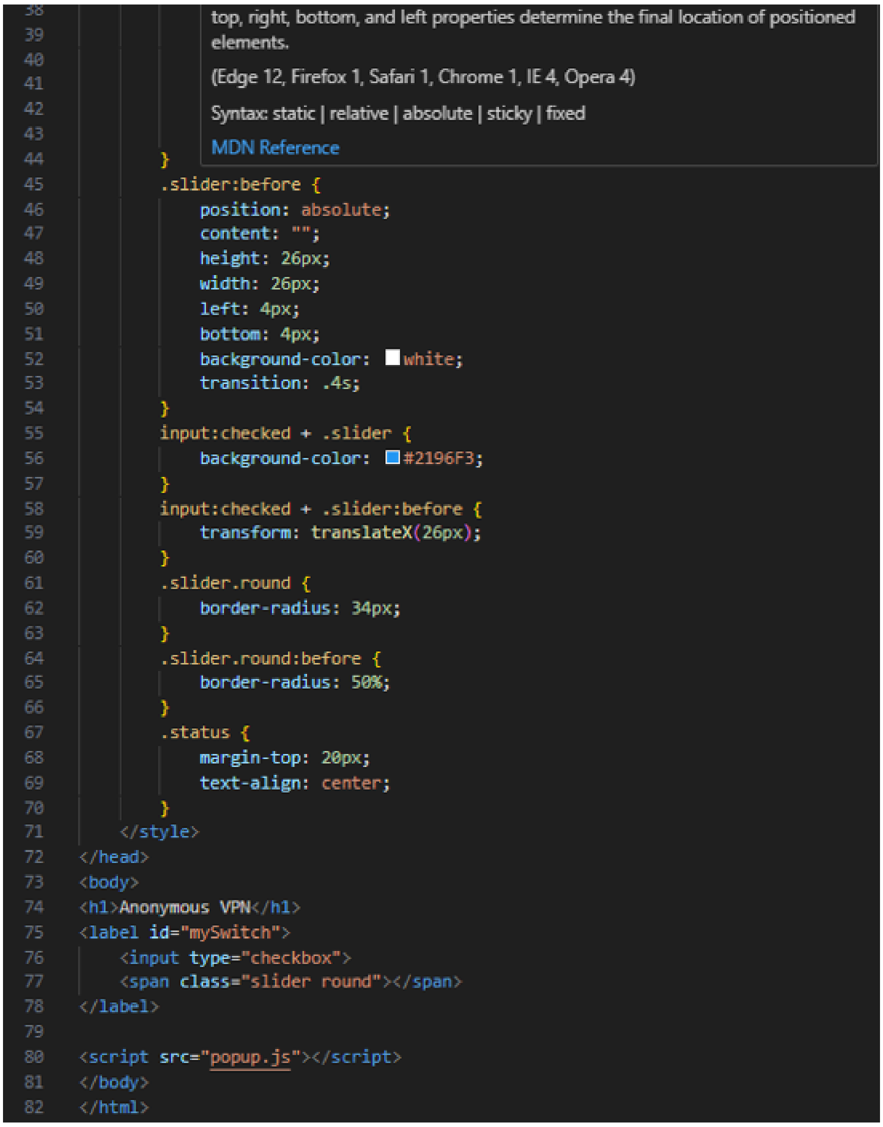
```
if (typeof browser === "undefined") {
    var browser = chrome;
};
function openTab(){

    var newTab = browser.tabs.create({
        url:'https://twitter.com',
        active:true
    })
}

browser.browserAction.onClicked.addListener(openTab)
```

Figure 5.2: background script



```
<!DOCTYPE html>
<html>
<head>
    <style>
        body {
            display: flex;
            justify-content: flex-start;
            align-items: center;
            width: 400px;
            height: 400px;
            padding: 10px;
            background-color: black;
            color: white;
            flex-direction: column;
        }
        h1 {
            font-size: 2em;
            margin: 0;
            padding: 0;
            width: 100%;
            text-align: center;
            margin-bottom: 20px;
        }
        #mySwitch {
            position: relative;
            display: inline-block;
            width: 60px;
            height: 34px;
        }
        #mySwitch input {
            opacity: 0;
            width: 0;
            height: 0;
        }
        .slider {
            position: absolute;
            cursor: pointer;
            top: 0;
            left: 0;
```

Figure 5.3: html File



top, right, bottom, and left properties determine the final location of positioned elements.

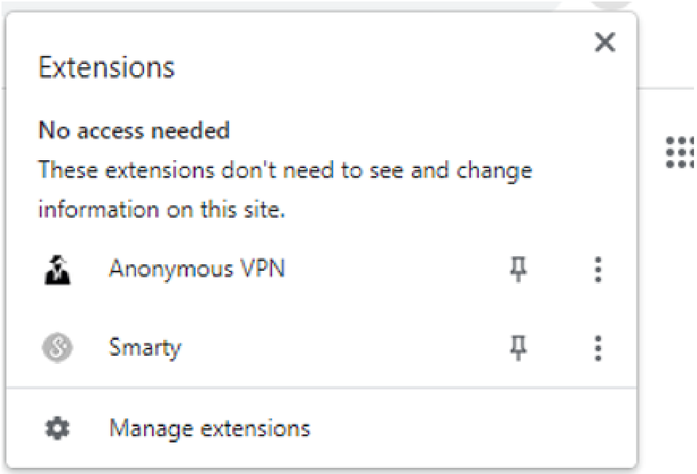
(Edge 12, Firefox 1, Safari 1, Chrome 1, IE 4, Opera 4)

Syntax: static | relative | absolute | sticky | fixed

MDN Reference

```
        }
        .slider:before {
            position: absolute;
            content: "";
            height: 26px;
            width: 26px;
            left: 4px;
            bottom: 4px;
            background-color: white;
            transition: .4s;
        }
        input:checked + .slider {
            background-color: #2196F3;
        }
        input:checked + .slider:before {
            transform: translateX(26px);
        }
        .slider.round {
            border-radius: 34px;
        }
        .slider.round:before {
            border-radius: 50%;
        }
        .status {
            margin-top: 20px;
            text-align: center;
        }
    </style>
</head>
<body>
<h1>Anonymous VPN</h1>
<label id="mySwitch">
    <input type="checkbox">
    <span class="slider round"></span>
</label>

<script src="popup.js"></script>
</body>
</html>
```

Figure 5.4: html file-2



Extensions

No access needed

These extensions don't need to see and change information on this site.

Figure 5.5: Extension added to chrome

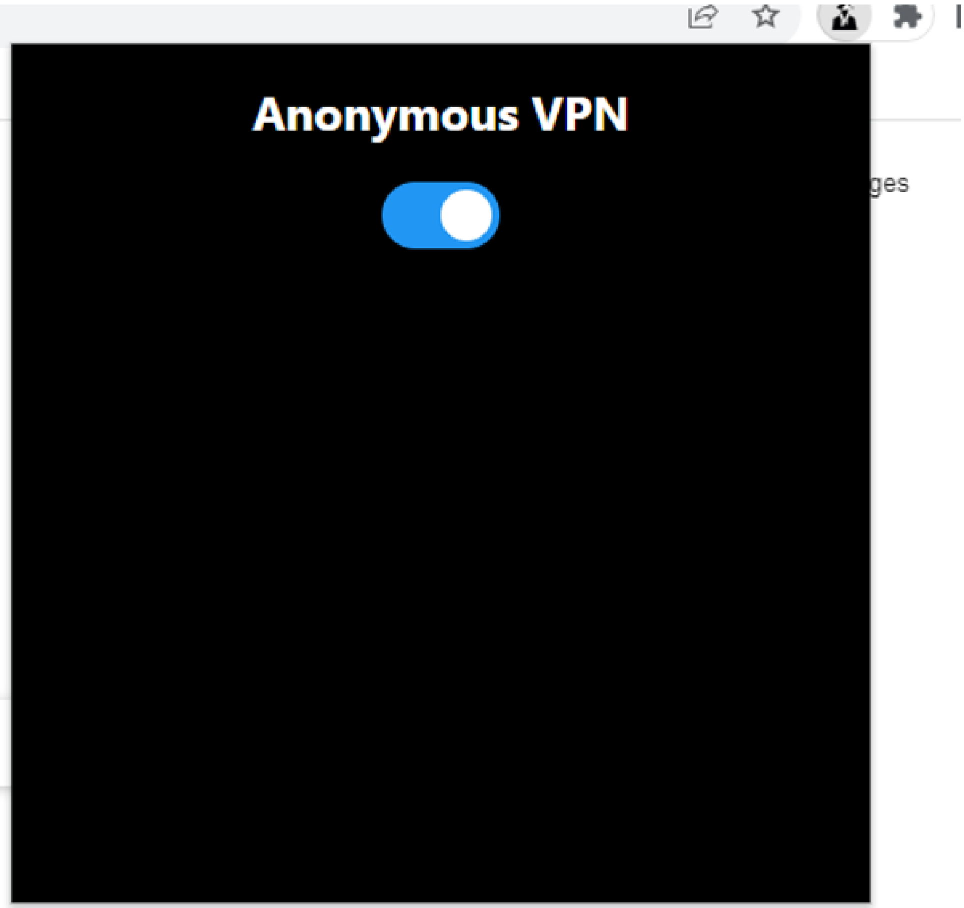


Figure 5.6: Initial UI of VPN popup

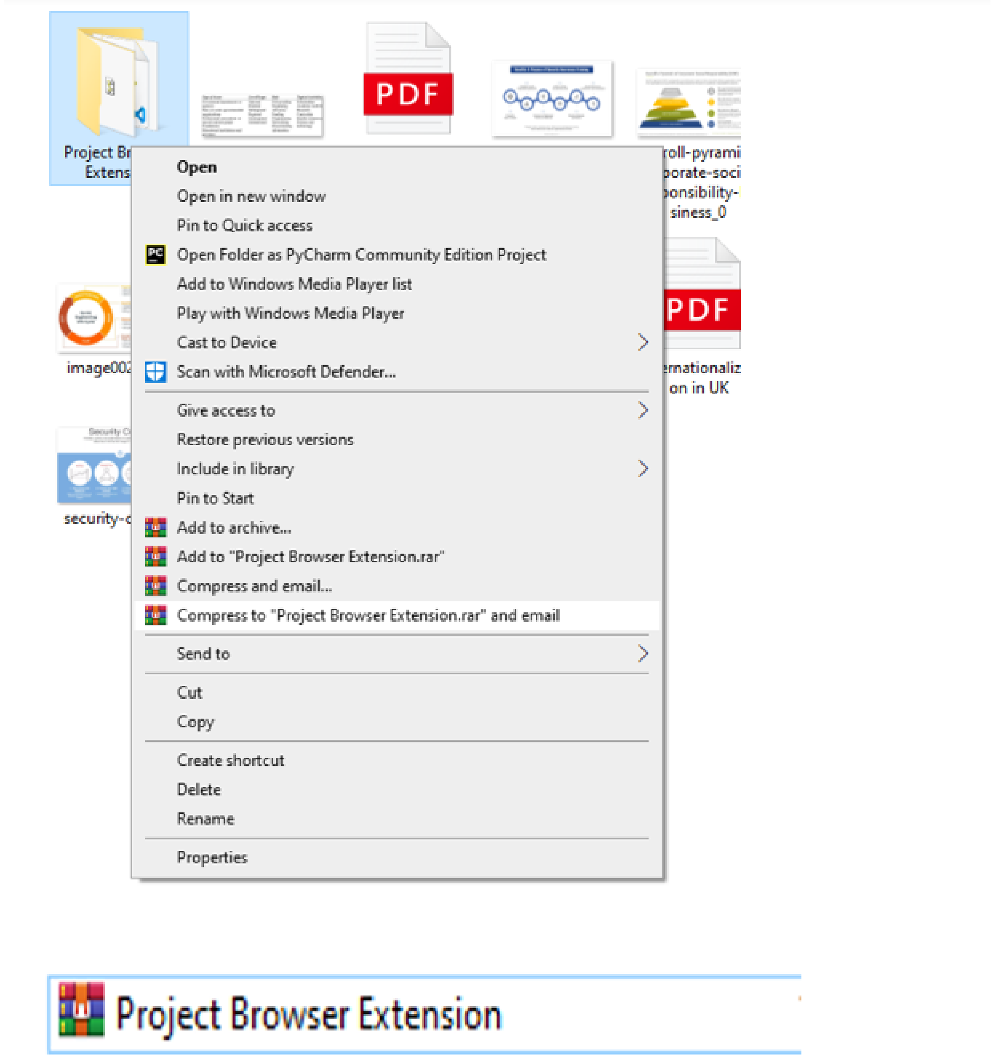


Figure 5.7: Compressing and Compressed

was a huge improvement. Several features were added to the user interface (UI) of the browser plugin to improve the user experience and give it a more professional look.

The inclusion of a nation choice inside the popup UI was a crucial improvement. Users were able to choose exactly which country they wanted to connect to their VPN server with this function. Additionally, a ground-breaking option called "Random" was made available inside the dropdown menu, allowing the plugin to independently create a VPN connection to a server that was selected at random from any location in the globe.

A connection status indicator was included into the popup UI to provide transparency and user knowledge. This provided customers with quick information about the state of their surfing privacy by clearly communicating whether the VPN connection was active or not.

The addition of a toggleable connection button allowed for more user control. This button gave users the freedom to quickly enable or disable the VPN connection as needed to meet their urgent privacy requirements.

Through skillful use of CSS styles and design principles, the UI's aesthetic appeal and usability were improved. This included a consistent stylistic strategy for buttons, drop down menus, and other UI components. In order to provide a consistent and smooth experience across a variety of screen sizes and devices, a thorough emphasis on responsive design was maintained.

By using clear icons and labels, the UI's usability was improved, making it easier for users to understand and navigate the plugin's interface. Notably, CSS was essential in personalizing error messages and feedback indications, providing a user-friendly strategy for dealing with future problems.

A smooth and user-friendly browser plugin was created as a consequence of the integration of the OpenVPN API connection, the extension of the UI with the country option and random selection functionality, and the strategic use of CSS style. Users were given the ability to create secure VPN connections that were customized to their tastes thanks to this all-encompassing strategy, enhancing their online privacy protections while through the digital world.

This is the Final Look of my Plugin I name it as **“Anonymous VPN"** (Fig 5.8, Fig 5.9).

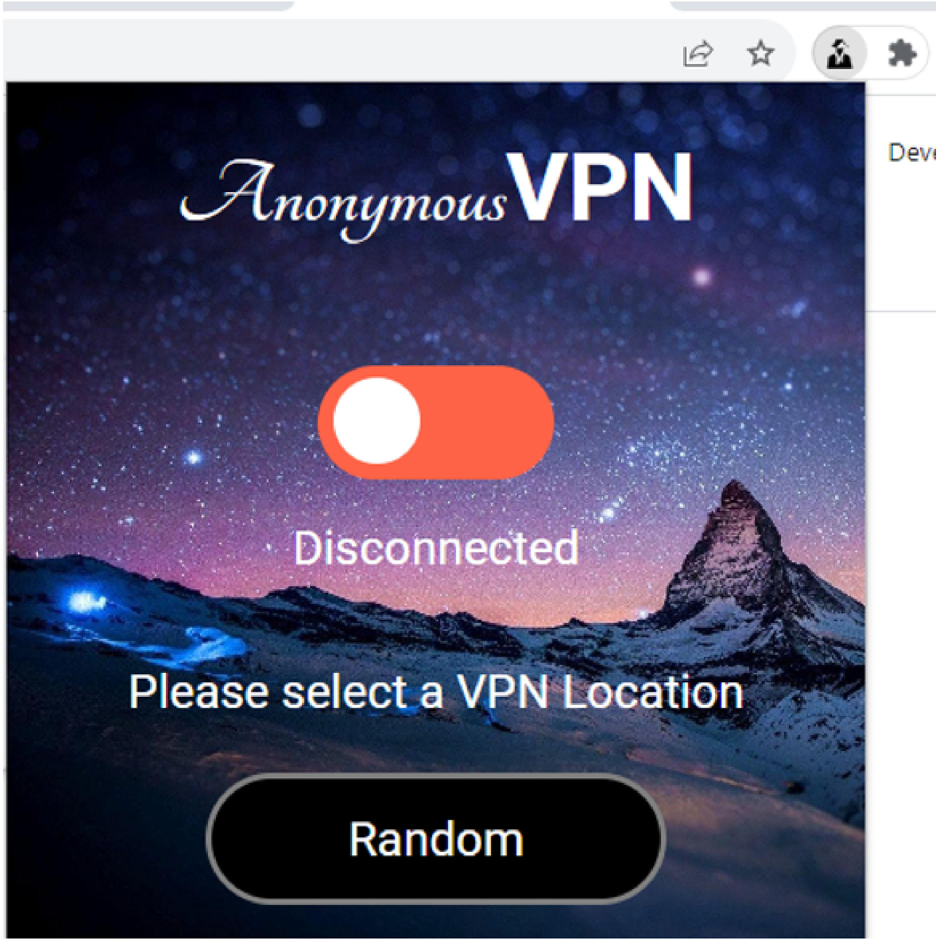


Figure 5.8: Final Look of VPN popup

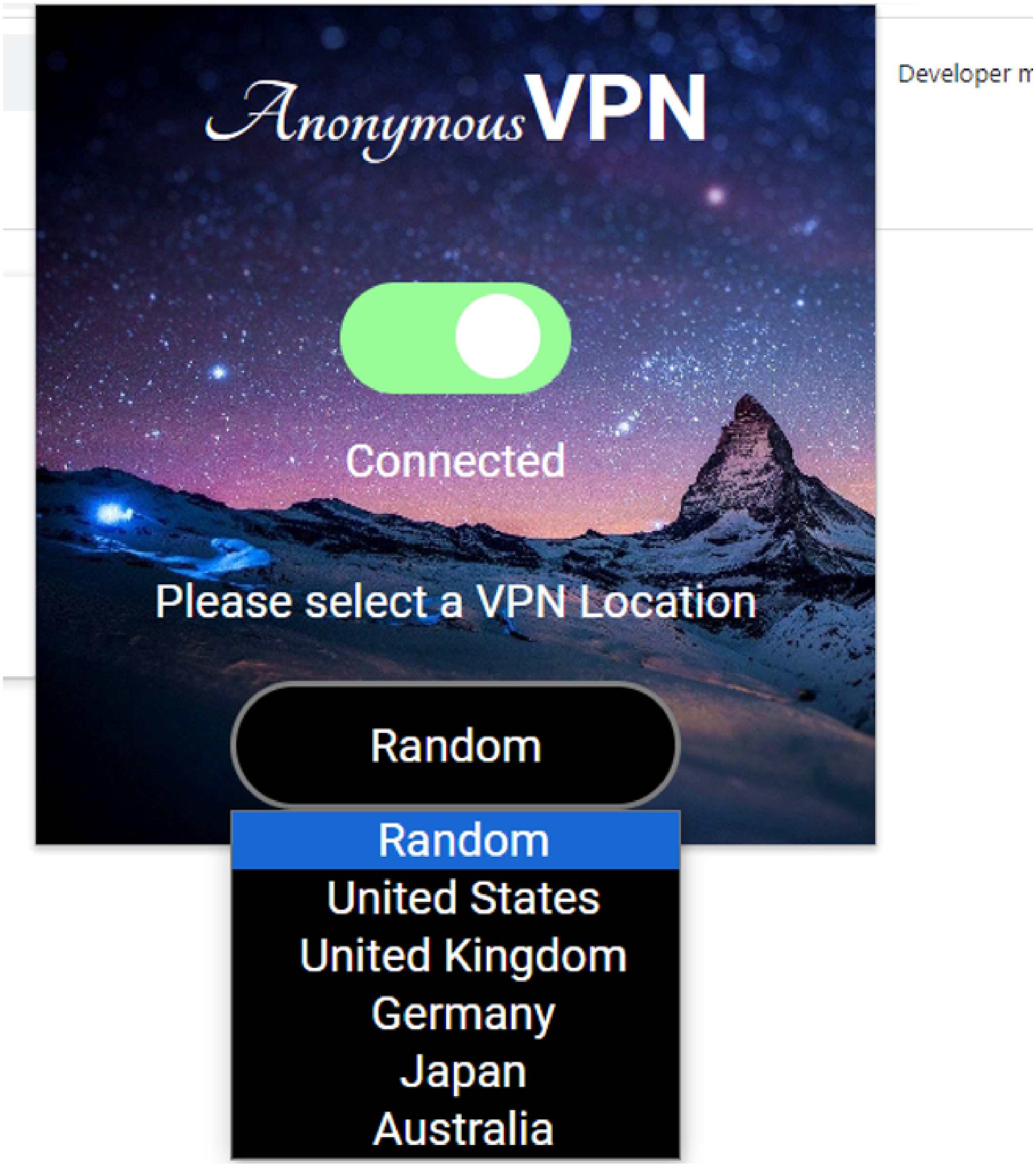


Figure 5.9: VPN connection countries

Chapter 6

Challenges and Difficulties

The implementation of the VPN component presented the project with a number of hurdles and difficulties during the development process.

The following things provided big challenges:

6.1 Availability of Appropriate APIs

Finding a suitable API that could support VPN connections proved to be the main problem Iran across during the project's development. In our original strategy, I searched extensively and thoroughly for APIs that would provide the needed VPN connectivity. In our search for a useful API solution, I perused numerous publications, online discussion boards, and repository sites. Unfortunately, the bulk of the publicly accessible APIs I came across were no longer in use and/or deprecated, making them inappropriate for the needs of our project.

Due to this setback, I looked into alternative solutions and got in touch with many VPN service providers. Our goal was to obtain temporary API access from these providers so that our browser plugin could allow the required VPN connections. Despite our best efforts, these attempts proved difficult because VPN service providers only sometimes and slowly responded to our requests. Even while some providers did ultimately reply, the general feeling was that giving us access to their API did not fit with their present business priorities.

Even well-known open-source alternatives, like OpenVPN, were investigated in our search for a workable API solution. However, I found that rather than providing the essential functioning VPN connections, the OpenVPN API mostly concentrated on access control methods. This served to highlight the dearth of marketable APIs that could meet the goals of our project.

I persevered in our search for viable API solutions in the face of these obstacles. In search of ideas and prospective directions for integrating API connectivity, Investigated existing VPN extensions. The "Touch VPN" add-on stood out as a remarkable example among these. I was unable to accomplish the goal of creating VPN connections within our browser plugin due to the persistent problem of unavailable or deprecated APIs.

I set out on a proactive journey of discussion with numerous VPN service providers in our search for a suitable API solution to enable VPN access within our project. This required contacting numerous respected service providers in the sector in an effort to obtain API access that would satisfy the needs of our project. However, I encountered number of challenges to move forward with my project.

6.2 Lack of Support and response

The lack of responsiveness from certain VPN providers was one of the greatest problems Iran into. Although I made a conscious effort to foster communication and outline the details of our program, delays and a lack of participation continued. I found it more challenging to advance and swiftly obtain the API access I required as a result.

When answers finally manifested, the outcomes were not always favorable. Some companies were reluctant to grant us access to their APIs, stating that doing so would conflict with their current business goals. Our project suffered greatly as a result because I was unable to establish the necessary VPN connectivity. This comprehension of the providers' point of view highlighted the precarious equilibrium between technology options and business considerations.

The fact that API access did not align with their business objectives was a glaring example of the challenges that businesses face when choosing their alliances and collaborations. It became clear that although the goal of our project was to increase user privacy and security, the economic environment of the VPN sector had a significant impact on how easily accessible the necessary APIs were.

Finding partners who have the same values and ambitions was further emphasized by this experience. Additionally, it demonstrated the constraints that outside developers can encounter when attempting to combine their projects with exclusive systems or services.

The difficulties I faced in securing API access were considerable, but they also provided insight into the complex relationships between corporate needs and technology advancement. The experience has highlighted the difficulty in bridging the gap between technological innovation and business realities and deepened our awareness of the need for careful alignment between project objectives and the interests of possible collaborators.

6.3 OpenAPI Limitations

I targeted the OpenVPN API in our search for workable API alternatives because of its open-source status and potential compatibility. However, it became clear from further investigation that the OpenVPN API did not meet the functional specifications of our project. The main issue Iran into was that the OpenVPN API mostly concentrated on access control techniques rather than providing the necessary functionality to set up a usable VPN connection.

The management of access rights and permissions for users within a network appears to be the focus of the OpenVPN API. Once the OpenVPN software was installed, it allowed for the control of who may access the VPN network. However, this specific functionality did not address the main goal of our project, which was to make it possible for customers to create VPN connections for more privacy and security when accessing the internet.

A major limitation was the absence of a way within the OpenVPN API to begin a VPN connection to a distant server. The API was unable to meet the demands of our project because it lacks the ability to create and maintain VPN connections programmatically. Despite being a trustworthy and open-source solution, OpenVPN's API was insufficient for the essential features I wished to build.

Because of this, and despite the potential advantages of using an open-source solution like OpenVPN, the API was not appropriate for our project due to its intrinsic focus on access control rather than practical VPN connection management. This finding further emphasized the significance of matching an API's technical capabilities to the project's goals and demonstrated that even open-source solutions can have drawbacks that should be carefully taken into account during the evaluation stage.

6.4 Deprecated and unsupported APIs

I faced a significant obstacle in the form of deprecated and unsupported options in our search for open-source VPN APIs that could be able to meet the needs of our project. I came up an obsolete version of NordVPN's API among these, which made us wonder about its applicability and functionality to our project. The versions of these deprecated APIs have undergone significant modifications or are no longer being actively maintained by their developers, making them unsuitable for inclusion into our project.

Deprecated APIs' compliance with current technology and security norms is their main problem. These APIs may be missing essential security updates and functionality needed to guarantee a safe and dependable VPN connection because they are no longer being regularly updated. This raises serious questions about how practical they would be for a project that seeks to improve user privacy and security by utilizing cutting-edge technologies.

APIs that are not supported by their developers lack continuing technical support and troubleshooting tools. This implies that there would be no official channels for requesting support or resolving issues in the event of technical difficulties or compatibility concerns. The availability of unsupported APIs considerably increased the danger of running into obstacles that could slow down or jeopardize the development process for our project, which required a solid and trustworthy API solution.

The discovery of these obsolete and unsupported APIs emphasizes how critical it is to use APIs that are supported actively and adhere to current industry standards. A good and secure implementation depends on access to the newest features, security upgrades, and technical assistance, all of which can be obtained by integrating such APIs. It also serves as a reminder of the dynamic nature of technology, where quick upgrades and developments can quickly make APIs that were once useful obsolete.

This example highlights the importance of thorough investigation and assessment when considering the incorporation of APIs into projects. It also emphasizes how crucial it is to look for APIs from reliable vendors who have a track record of dedication to continuous improvement and support. This understanding prompted us to concentrate our efforts on finding API solutions for our project that are not only practical but also resistant to the quick pace of technological change.

6.5 Limited Access to source code

During the developmental stage of the project, I recognized the significance of analyzing preexisting VPN extensions in order to acquire valuable insights and potentially exploit their functionalities. Nevertheless, our endeavors were impeded by a notable hindrance - limited availability of the development-level source code for these extensions. The limited access presented certain constraints on our capacity to fully comprehend the complexities of their internal mechanisms.

After conducting additional investigation, I successfully obtained access to a version of the extension's source code that was situated in the localappdata (with two percentage simple starting and ending) directory. Nevertheless, the code obtained was not sourced from the developmental stage; rather, it comprised the code for the production build. This posed a difficulty, as the code used in the production build is commonly compressed and transformed to enhance efficiency. The code that has been optimized did not possess a structure that was easily comprehensible, thereby hindering our ability to fully understand the functionalities of the extension.

Due to the limited timeframe of our project, the endeavor of deciphering the extension's functionalities from obfuscated and transformed code proved to be exceedingly challenging. Deciphering the underlying logic and mechanics of the extension proved to be challenging due to the lack of well-defined code structures, meaningful variable names, and explanatory comments.

Notwithstanding our diligent endeavors to acquire knowledge from extant VPN extensions, the task of reverse engineering has highlighted the complex intricacies involved in deciphering code at the level of production. The significance of having access to development-level source code becomes evident when considering the intricacies brought about by magnification and transpilation, as it aids in comprehending and potentially incorporating features from pre-existing extensions.

In essence, the limited availability of the source code at the development level serves as a poignant reminder of the proprietary characteristics inherent in software development. The statement emphasized the importance of comprehensive documentation, appropriate version control, and transparent code sharing practices within the software development community. The difficulties encountered in the field of reverse engineering were significant, serving as a reminder of the importance of transparency and collaboration within the software development domain. These factors are crucial in promoting the exchange of knowledge and fostering innovation.

6.6 Similar VPN Extension

I discovered the "Touch VPN" extension during our research of available VPN extensions because it seemed to fit our project's objectives the best. This revelation first generated excitement since the attributes of the extension looked to align with the goals of improving user privacy through VPN technology. But as I dug more, a major obstacle became apparent: there was no working API that could meet the precise specifications of our project.

The "Touch VPN" plugin showed many parallels to our approach, including its focus on boosting user privacy and security while engaging in online activities. This congruence gave us hope that our initiative was not unique in its efforts to leverage VPN technology to protect user information. The similarities between our idea and the "Touch VPN" extension gave us optimism that I might be able to learn something or be inspired by their strategy.

But the absence of a useful API to enable VPN connectivity remained the main issue in both projects. The "Touch VPN" add-on offered insightful suggestions and viewpoints on how to improve privacy and create user interfaces, but it did not address the core need for creating VPN connections using an API. This difficulty brought to light the necessity for an accessible and useful API solution, a problem that projects attempting to use VPN technology within browser extensions frequently encounter.

Although our project and the "Touch VPN" extension have certain similarities, the lack of a suitable API highlighted the critical role that API availability plays in achieving the needed functions. This typical constraint highlighted the significance of a trustworthy and well-documented API for successfully integrating cutting-edge technologies into browser extensions.

In conclusion, learning about the "Touch VPN" extension gave us important new information about how our project's objectives matched up with those of already-existing programs. The lack of a usable API, however, continued to be the major problem. This experience served as a reminder of the importance of API functionality and accessibility, as well as the fact that even projects with similar goals may encounter difficulties if essential technological components are missing.

Despite these significant setbacks, the project's overall goal—the unrelenting dedication to improving user privacy and security in the digital sphere—remains unshakable. The foundation, research, and development phases of the project demonstrated an unwavering commitment to tackling the urgent issues of online monitoring and profiling. The difficulties encountered along the way only emphasized how urgent it is to establish an atmosphere that is supportive of API availability and collaboration, as these factors have an impact that goes well beyond the scope of individual projects, influencing the landscape of technological advancements and ensuring user experiences on a larger scale.

Chapter 7

Finding and Analysis

The identification and evaluation of suitable solutions played a pivotal role in shaping the course of this project. The process encompassed a complex and meticulous exploration of focused efforts with the objective of identifying a practical API solution that could effectively enable VPN connectivity, while seamlessly aligning with the overarching objectives of the project. The primary objective of these endeavors was to ascertain an Application Programming Interface (API) that could seamlessly integrate into the structure of the browser plugin, providing users with the envisioned Virtual Private Network (VPN) connections with optimal smoothness and effectiveness.

A thorough analysis of the many regions where well-known providers offer virtual private network (VPN) services was conducted.

The quest for a viable API solution involved a thorough evaluation of all options. Application programming interfaces (APIs) provided by reputable virtual private network (VPN) service providers were thoroughly evaluated as part of the study, and OpenVPN and other open-source projects were also looked into. The purpose was to thoroughly evaluate the possible synergies between these application programming interfaces (APIs) and the project's goals of incorporating virtual private network (VPN) connectivity into the browser plugin. The occurrence brought to light a challenge that emerged in the form of outdated and unsupported application programming interfaces (APIs), a barrier that had a substantial influence on the project's course.

Upon closer examination, it became evident that many of the APIs initially perceived as appealing were either outdated or lacked adequate support, leading to a disappointing realization. The deprecated application programming interfaces (APIs), which initially showed potential, have become incongruous with the swiftly changing technological environment. The issue was further exacerbated by incompatibilities with the prerequisites of the project, which limited the feasibility of integrating VPN connectivity as originally envisioned.

This statement emphasizes the inherent dynamism and constantly evolving characteristics of technology. The rapid progress in the field of technology frequently renders previously reliable solutions obsolete. The analysis demonstrated that the pursuit of API solutions necessitates an ongoing diligence in discerning APIs that are not only pertinent but also consistently updated. The success of the project relied on the incorporation of sophisticated VPN technology, and this obstacle emphasized the importance of partnering with up-to-date and adaptable APIs.

The recognition of the crucial significance that current and well-maintained application programming interfaces (APIs) holds in technological integrations became apparent. The rapid advancement of technology necessitates a strong integration with regularly updated and supported

APIs to maintain the long-term functionality and security of projects. Given the existence of outdated and unsupported application programming interfaces (APIs), the project was motivated to approach the situation with increased discernment, placing significant importance on establishing collaborations with APIs that align with the project's dynamic nature and dedication to innovation.

The act of engaging in communication endeavors with VPN service providers provided a deeper understanding of the complex landscape within the industry. The interactions provided a plethora of valuable insights pertaining to the field of VPN technology, thereby illuminating potential opportunities for collaboration. Nevertheless, this stage of the project was characterized by various obstacles that brought attention to the complex nature of obtaining access to external application programming interfaces (APIs).

The occurrence of response delays has been identified as a notable impediment in the communication process. Efforts were undertaken to cultivate a harmonious relationship with VPN service providers; however, the delay in receiving timely responses impeded the progress of the project. The delays highlight the intricacies involved in coordinating partnerships within the technology sector, where timely communication plays a crucial role in achieving project deadlines and goals.

Moreover, the issue of restricted compatibility with the objectives of the project introduced an additional level of intricacy. Not all instances of communication exchanges yielded a flawless congruence between the capabilities of the application programming interfaces (APIs) provided by service providers and the desired functionality of the project. This finding illustrates that the diversity of APIs necessitates careful evaluation to ensure their compatibility with the specific integration needs.

One notable observation that arose from the collected responses was the expression of reservations by certain providers regarding the sharing of their application programming interfaces (APIs). The underlying justification frequently revolved around a strategic determination rooted in commercial considerations. This elucidated the complex dynamics between technological collaborations and business tactics within the technology ecosystem. The necessity to achieve a harmonious alignment between innovation and business objectives became evident, underscoring the crucial nature of harmonizing interests for the successful collaboration of APIs.

The thorough examination of the data obtained from the API search and communication phase led to a significant revelation: the key factor for the project's effective implementation relied on the availability of strong and reliable APIs. The application programming interfaces (APIs) served as the fundamental foundation on which the entire project's functionality relied. Due to the lack of these application programming interfaces (APIs), the project is more vulnerable and their critical role in fostering innovation and facilitating seamless integration is highlighted.

This analysis emphasized a fundamental fact even more: there are differences in the capabilities and quality of various APIs. Since the project's goals were complex and specific, it was necessary to use application programming interfaces (APIs) that closely matched the intended functionalities, security protocols, and compatibility requirements. The results showed that choosing application programming interfaces (APIs) was important since they were the link between the theoretical framework and its actual implementation.

The difficulties faced during this phase have also brought to light a more thorough understanding: the requirement for flexibility and agility when negotiating the complexities of the technical world. Technology is characterized by constant evolution, with many different aspects having the ability to have an impact on other fields. These difficulties served as a potent reminder of the value of being well-prepared for projects to be able to change and adapt techniques as necessary.

The knowledge gathered from the project emphasizes how important it is to manage external dependencies strategically and wisely to succeed in technical endeavors. The assertion demonstrates how application programming interfaces (APIs) can be utilized for purposes other than their fundamental functionality. It considers things like security, compatibility, and flexibility. The challenge the team faced in locating the ideal API served as a timely reminder of the necessity to keep an open mind, make wise decisions, and approach issues head-on. These strategies are crucial for ensuring the success of upcoming technological endeavors.

In conclusion, finding and evaluating application programming interfaces (APIs) acts as an effective reminder of the intrinsic importance of these components within the context of project development. Application Programming Interfaces (APIs) are essential to the realization of groundbreaking ideas, as our expedition has revealed. These variables have an impact on how functionality is chosen, security paradigms are shaped, and technologies are seamlessly included into a project's architecture. This finding emphasizes how important careful API selection is, as it has a significant impact on how technological efforts develop.

This expedition additionally provides substantiation of the intricate obstacles entailed in accessing application programming interfaces (APIs) from diverse origins. The expedition unveiled a diverse landscape marked by outdated decisions, elusive responses, and the complex interplay between technological progress and commercial considerations. These findings provide insight into future directions, underscoring the significance of meticulously crafted selection criteria, adaptable flexibility, and strategic partnerships. In summary, this study underscores the crucial role of APIs in enabling innovation, emphasizing the importance of effectively managing their scope to ensure the smooth integration of cutting-edge technologies in future endeavors.

Chapter 8

Conclusion

As this project ends, a compelling narrative emerges that paints a vivid image of its essential qualities, the challenges it faced, and the admirable goals it aimed to accomplish. The road made to deploy randomized VPN connections via a browser plugin to increase user privacy has provided a plethora of priceless insights and lessons that capture the limitless possibilities of innovation and the complex geography of technology landscapes.

The core of the project is its dedication to enhancing user privacy, a subject of utmost significance in our technologically advanced society. The project aimed to provide users more control over their online experiences by inventing the integration of randomized VPN connections within a browser plugin, sheltering them from intrusive tracking technologies, and protecting their data from potential vulnerabilities. The project's core values are in line with the widespread call for stronger data protection and cybersecurity measures.

However, the road to success was not without its difficulties, demonstrating the complexity of contemporary technological endeavors. The project faced challenges in looking for appropriate APIs, negotiating communication challenges with VPN service providers, and addressing compatibility and security issues. These difficulties revealed the intricate mosaic of actual technological difficulties and their integration into project development, far from being deterrents.

The project gained deep understanding along the way that shed light on the beneficial interaction between innovation and the complexity of the technical landscape. The significance of careful API selection, the art of fluid communication with outside providers, and the requirement for quick adaptation to constantly changing technologies all came to the fore. The entire project stands for a comprehensive awareness of the complex dance between ideas and their materialization, not merely the pinnacle of code and development.

The progress of this project shed light on the crucial position that Application Programming Interfaces (APIs) play in the process of shaping project development. Finding the proper APIs was likened to unravelling a complex tapestry because there were so many alternatives available (49). The pursuit underlined APIs' paramount significance in achieving project goals, from the variety of deprecated options that still had some residual usefulness to the potential for forming partnerships with VPN providers.

The difficulties encountered in this endeavor served as stark reminders of the ever-evolving nature of technology. These difficulties evolved into poignant symbols of the dynamic environment in which technology functions. The difficulties of working with VPN service providers and the experiences with deprecated choices highlighted the necessity for APIs that are not only functionally compatible but also flexible to changing security standards and compatibility requirements.

In addition to difficulties, the search for appropriate APIs revealed a thorough awareness of the complex interactions between technology and business strategy. The attempts to communicate with VPN service providers have highlighted the delicate balance that must be struck between forming technological alliances and defending commercial interests. The disclosures served as a stinging reminder that the world of technology is intimately intertwined into the larger fabric of business goals rather than being in a vacuum.

Without a doubt, the challenges and difficulties faced along the way have not altered the project's original goals. The possibility to empower users with specialized VPN connections is represented by the incorporation of the OpenVPN API in the future. A user experience that goes beyond functionality to give ease and transparency is promised with the addition of features like the country dropdown and random server selections, in combination with a connection status indicator (50).

The project's goals are materialized through the painstaking design of the plugin's user interface. A transformative force emerges from the shadows of more technical considerations: CSS styling. With skillful style, the plugin's user interface (UI) moves beyond its functional purpose and transforms into an aesthetic treat, showcasing a visually appealing and responsive design that complies with current web standards.

In the future, this project isn't only about overcoming obstacles; it's a little representation of the difficulties supporting modern technology advancements. Perseverance emerges as the underlying theme throughout the complex web of API searches, service provider discussions, and compatibility issues. The trip highlights the importance of adaptability and the capacity to navigate the constantly altering technological landscape while upholding an unflinching dedication to innovation's lofty aspirations.

As this phase ends, the project serves as both an homage to technological prowess and the spirit of exploration itself. It calls on everyone who interacts with it to recognize the complex relationship between technology and business and to warmly welcome innovation's dynamic nature. Beyond the lines of code and the UI upgrades, this project is an invitation for everyone to work together to create a digital environment that protects user privacy and represents the unrelenting march of development towards a more inclusive and secure digital future.

8.1 Limitations

The constraints that have affected the project's scope and development cover a number of important areas:

API Unavailability: One major drawback has been the absence of a reliable API for creating VPN connections. Despite thorough searches, many publicly available solutions were either out of date or didn't meet the project's functional needs.

Dependence on Third-Party Services: Using outside VPN service providers to access their APIs brought uncertainty. The project's dependence on outside elements was highlighted by providers' discretion in allowing access and their delays in responding.

Limited Control Over VPN Infrastructure: The project was unable to directly control VPN infrastructure, which had an impact on the customization and optimization of VPN connections, because there was no working VPN API.

Although the project intends to increase privacy, its reliance on third-party VPN providers raises concerns about the security of user data within those services.

Challenges in Reverse Engineering: Being restricted to production build code and having limited access to development-level source code made it difficult to have a thorough grasp of the extension possibilities already in place.

Ambitious aims within a constrained timeline may affect thorough implementation, testing, and the investigation of alternate alternatives. Project scope and time constraints.

Together, these restrictions offer a comprehensive understanding of the project's difficulties and the environment in which it takes place.

8.2 Future work

The project has the potential to evolve in a number of crucial ways in the future. First and foremost, it is imperative to keep looking for a VPN API that is both functional and compatible with the project's objectives. This could entail investigating cutting-edge technology, working with VPN providers, or even thinking about creating a private API. The project's functionality is based on the presence of a trustworthy API.

The development of privacy features is another potential area for future effort. This might involve putting advanced privacy-preserving measures into practice, such better cookie management and more sophisticated content filtering mechanisms. The project's effectiveness in enhancing privacy can be greatly increased by strengthening the plugin's capacity to protect user data and minimize tracking technologies.

Additionally, improving user experience is a crucial factor. This calls for both functional and aesthetically pleasing improvements. The adoption rate of the plugin could rise as a result of making improvements to the user interface's design, usability, and interactivity since consumers may perceive it to be more logical and aesthetically pleasing.

Future development must also prioritize performance optimization. Users can have a better and more productive browsing experience by reducing latency, optimizing connection formation procedures, and making sure the plugin works without a hitch.

Security continues to be a major problem. To make sure user data is kept safe and secure, thorough security audits, vulnerability analyses, and assuring adherence to the highest security requirements are ongoing activities.

The popularity of the plugin may also be greatly influenced by activities to increase education about online privacy and to encourage the use of the plugin. This can entail developing guides, classes, or other materials that inform users about the value of privacy and the ways in which the plugin might improve their online safety.

Appendix A

Test code - Popup.js

```
document.addEventListener("DOMContentLoaded", function()
    document.querySelector("mySwitch input").addEventListener("change", function()
    var statusText = document.querySelector(".status");
    if (this.checked)
    console.log("Switch is ON");
    statusText.textContent = "Connected";
    // Save the state to chrome.storage
    chrome.storage.sync.set(switchState: true, function()
    console.log(’Switch state is set to ’ + true);
    );
    else
    console.log("Switch is OFF");
    statusText.textContent = "Disconnected";
    // Save the state to chrome.storage
    chrome.storage.sync.set(switchState: false, function()
    console.log(’Switch state is set to ’ + false);
    );
    );
    // On startup, check the saved state and update the switch
    chrome.storage.sync.get(’switchState’, function(data)
    document.querySelector("mySwitch input").checked = data.switchState;
    document.querySelector(".status").textContent = data.switchState ?
    "Connected" : "Disconnected";
    );
    );
```

Appendix B

Test code - main.js

```
console.log("The extension is up and running");
```

Appendix C

Test code - popup.html

```
<!DOCTYPE html>
    <html>
    <head>
    <link href="https://fonts.googleapis.com/css2?
    family=Tangerine:wght@700family=Roboto:wght@400;700display=swap" rel="stylesheet">
    <style>
    body
    display: flex;
    justify-content: flex-start;
    align-items: center;
    width: 400px;
    height: 400px;
    padding: 10px;
    background-image: url(’349872.jpg’);
    background-size: cover;
    color: white;
    flex-direction: column;
    h1
    font-size: 4em;
    margin: 0;
    padding: 0;
    width: 100
    text-align: center;
    margin-bottom: 60px;
    h1 span
    font-family: ’Roboto’, sans-serif;
    font-weight: 700;
    mySwitch
    position: relative;
    display: inline-block;
    width: 120px;
    height: 60px;
```

```
mySwitch input
opacity: 0;
width: 0;
height: 0;
.slider
position: absolute;
cursor: pointer;
top: 0;
left: 0;
right: 0;
bottom: 0;
background-color: FF6347;
transition: .4s;
.slider:before
position: absolute;
content: "";
height: 44px;
width: 44px;
left: 8px;
bottom: 8px;
background-color: white;
transition: .4s;
input:checked + .slider
background-color: 98FB98;
input:checked + .slider:before
transform: translateX(52px);
.slider.round
border-radius: 30px;
.slider.round:before
border-radius: 50
.status
margin-top: 20px;
text-align: center;
font-size: 2em;
font-family: 'Roboto', sans-serif;
.vpn-text
margin-top: 20px;
text-align: center;
font-size: 2em;
font-family: 'Roboto', sans-serif;
select
margin-top: 3px;
```

```
font-size: 2em;
font-family: ’Roboto’, sans-serif;
color: white;
background-color: black;
border: 3px solid 808080;
border-radius: 34px;
padding: 10px;
outline: none;
width: 234px;
height: 68px;
appearance: none;
position: relative;
text-align: center; /* Center the text */
</style>
</head>
<body>
<h1><span style="font-family: ’Tangerine’, cursive; font-weight: normal;">Anonymous</span><span>VPN
<label id="mySwitch">
<input type="checkbox">
<span class="slider round"></span>
</label>
<p class="status">Disconnected</p>
<p class="vpn-text">Please select a VPN Location</p>
<select id="countrySelect">
<option value="random">Random</option>
<option value="us">United States</option>
<option value="gb">United Kingdom</option>
<option value="de">Germany</option>
<option value="jp">Japan</option>
<option value="au">Australia</option>
</select>
<script src="popup.js"></script>
</body>
</html>
```

Bibliography

[1] A. PET, J. Mikhail, and N. J. Hopper, “Privacy enhancing technologies: 10th international symposium, pets 2010, berlin, germany, july 21-23, 2010: proceedings,” *(No Title)*.

[2] A. A. M. Lehmoud, N. T. Obeis, and A. F. Mutar, “Proposing a security system for the vpn through design and implementation of a scheme for android and ios mobiles based on two-factor authentication,” *Periodicals of Engineering and Natural Sciences*, vol. 10, no. 2, pp. 292–303, 2022.

[3] A. Vastel, P. Laperdrix, W. Rudametkin, and R. Rouvoy, “{Fp-Scanner}: The privacy implications of browser fingerprint inconsistencies,” in *27th USENIX Security Symposium (USENIX Security 18)*, pp. 135–150, 2018.

[4] S. Jahan, M. S. Rahman, and S. Saha, “Application specific tunneling protocol selection for virtual private networks,” in *2017 international conference on networking, systems and security (nsyss)*, pp. 39–44, IEEE, 2017.

[5] F. Shahzad, “Modern and responsive mobile-enabled web applications,” *Procedia Computer Science*, vol. 110, pp. 410–415, 2017.

[6] H. Abbas, N. Emmanuel, M. F. Amjad, T. Yaqoob, M. Atiquzzaman, Z. Iqbal, N. Shafqat, W. b. Shahid, A. Tanveer, and U. Ashfaq, “Security assessment and evaluation of vpns: A comprehensive survey,” *ACM Computing Surveys*, 2023.

[7] M. Rodriguez-Garcia, M. Batet, D. Sánchez, and A. Viejo, “Privacy protection of user profiles in online search via semantic randomization,” *Knowledge and Information Systems*, vol. 63, pp. 2455–2477, 2021.

[8] K. K. Jyothi and B. I. Reddy, “Study on virtual private network (vpn), vpn’s protocols and security,” *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 3, no. 5, pp. 919–932, 2018.

[9] M. I. Zakaria, M. N. Norizan, M. M. Isa, M. F. Jamlos, and M. Mustapa, “Comparative analysis on virtual private network in the internet of things gateways,” *Indones. J. Electr. Eng. Comput. Sci*, vol. 28, no. 1, pp. 488–497, 2022.

[10] R. Bangar, V. Narkar, A. Phand, and J. Lohokare, “Catch me if you can: achieving complete internet anonymity using open source technologies,” 2022.

[11] A. Felfernig, G. Friedrich, D. Jannach, and M. Zanker, “Web-based configuration of virtual private networks with multiple suppliers,” in *Artificial Intelligence in Design’02*, pp. 41–61, Springer, 2002.

[12] A. Dutkowska-Zuk, A. Hounsel, A. Morrill, A. Xiong, M. Chetty, and N. Feamster, “How and why people use virtual private networks,” in *31st USENIX Security Symposium (USENIX Security 22)*, pp. 3451–3465, 2022.

[13] S. Khanvilkar and A. Khokhar, “Virtual private networks: an overview with performance evaluation,” *IEEE Communications Magazine*, vol. 42, no. 10, pp. 146–154, 2004.

[14] J. Kuo and C. M. Burns, “A work domain analysis for virtual private networks,” in *Smc 2000 conference proceedings. 2000 ieee international conference on systems, man and cybernetics.'cybernetics evolving to systems, humans, organizations, and their complex interactions'(cat. no. 0*, vol. 3, pp. 1972–1977, IEEE, 2000.

[15] K. Choudhary, K. Gupta, R. Chawla, P. Sharma, and M. Sharma, “Cloud computing service models: Traditional and user-centric approaches,” *Applications of Cloud Computing: Approaches and Practices*, p. 43, 2020.

[16] F. Farid, M. Elkhodr, F. Sabrina, F. Ahamed, and E. Gide, “A smart biometric identity management framework for personalised iot and cloud computing-based healthcare services,” *Sensors*, vol. 21, no. 2, p. 552, 2021.

[17] O. R. Hammoud and I. A. Tarkhanov, “A method to prevent tracking browsing history with the use of browser extension,” in *2019 4th International Conference on Computer Science and Engineering (UBMK)*, pp. 251–254, IEEE, 2019.

[18] R. Ramesh, L. Evdokimov, D. Xue, and R. Ensafi, “Vpnalyzer: systematic investigation of the vpn ecosystem,” in *Network and Distributed System Security*, pp. 24–28, 2022.

[19] J. T. Harmening, “Virtual private networks,” in *Computer and Information Security Handbook*, pp. 843–856, Elsevier, 2017.

[20] R. S. Ravindran, C. Huang, and K. Thulasiraman, “Managed dynamic vpn service: Core capacity sharing schemes for improved vpn performance,” in *2007 IEEE International Conference on Communications*, pp. 211–216, IEEE, 2007.

[21] J. Liu, Y. Li, N. Van Vorst, S. Mann, and K. Hellman, “A real-time network simulation infrastructure based on openvpn,” *Journal of Systems and Software*, vol. 82, no. 3, pp. 473–485, 2009.

[22] D. Barradas, N. Santos, L. Rodrigues, and V. Nunes, “Poking a hole in the wall: Efficient censorship-resistant internet communications by parasitizing on webrtc,” in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pp. 35–48, 2020.

[23] R. Ensafi, D. Fifield, P. Winter, N. Feamster, N. Weaver, and V. Paxson, “Examining how the great firewall discovers hidden circumvention servers,” in *Proceedings of the 2015 Internet Measurement Conference*, pp. 445–458, 2015.

[24] R. Younglove, “Virtual private networks-how they work,” *Computing & Control Engineering Journal*, vol. 11, no. 6, pp. 260–262, 2000.

[25] H. Gunleifsen, T. Kemmerich, and V. Gkioulos, “Dynamic setup of ipsec vpns in service function chaining,” *Computer Networks*, vol. 160, pp. 77–91, 2019.

[26] N. Kaaniche, M. Laurent, and S. Belguith, “Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey,” *Journal of Network and Computer Applications*, vol. 171, p. 102807, 2020.

[27] M. Ter Louw, J. S. Lim, and V. N. Venkatakrishnan, “Enhancing web browser security against malware extensions,” *Journal in Computer Virology*, vol. 4, pp. 179–195, 2008.

[28] A. X. Liu and F. Chen, “Collaborative enforcement of firewall policies in virtual private

networks," in *Proceedings of the twenty-seventh ACM symposium on Principles of distributed computing*, pp. 95–104, 2008.

[29] S. Y. Ameen and S. W. Nourildean, "Firewall and vpn investigation on cloud computing performance," *International Journal of Computer Science and Engineering Survey*, vol. 5, no. 2, p. 15, 2014.

[30] J. P. McGregor and R. B. Lee, "Performance impact of data compression on virtual private network transactions," in *Proceedings 25th Annual IEEE Conference on Local Computer Networks. LCN 2000*, pp. 500–510, IEEE, 2000.

[31] Z. Zhipeng, S. Chandel, S. Jingyao, Y. Shilin, Y. Yunnan, and Z. Jingji, "Vpn: a boon or trap?: a comparative study of mpls, ipsec, and ssl virtual private networks," in *2018 Second International Conference on Computing Methodologies and Communication (ICCMC)*, pp. 510–515, IEEE, 2018.

[32] O. Starov and N. Nikiforakis, "Privacymeter: Designing and developing a privacy-preserving browser extension," in *Engineering Secure Software and Systems: 10th International Symposium, ESSoS 2018, Paris, France, June 26-27, 2018, Proceedings 10*, pp. 77–95, Springer, 2018.

[33] D. Sánchez and A. Viejo, "Privacy-preserving and advertising-friendly web surfing," *Computer Communications*, vol. 130, pp. 113–123, 2018.

[34] E. Papadogiannakis, P. Papadopoulos, N. Kourtellis, and E. P. Markatos, "User tracking in the post-cookie era: How websites bypass gdpr consent to track users," in *Proceedings of the web conference 2021*, pp. 2130–2141, 2021.

[35] J. Samuel and B. Zhang, "Requestpolicy: Increasing web browsing privacy through control of cross-site requests," in *International Symposium on Privacy Enhancing Technologies Symposium*, pp. 128–142, Springer, 2009.

[36] M. Ikram and M. A. Kaafar, "A first look at mobile ad-blocking apps," in *2017 IEEE 16th International Symposium on Network Computing and Applications (NCA)*, pp. 1–8, IEEE, 2017.

[37] S. Ali, M. Elgharabawy, Q. Duchaussoy, M. Mannan, and A. Youssef, "Betrayed by the guardian: Security and privacy risks of parental control solutions," in *Annual Computer Security Applications Conference*, pp. 69–83, 2020.

[38] S. Carpenter, M. Shreeves, P. Brown, F. Zhu, and M. Zeng, "Designing warnings to reduce identity disclosure," *International Journal of Human–Computer Interaction*, vol. 34, no. 11, pp. 1077–1084, 2018.

[39] J. Bollen, H. Mao, and X. Zeng, "Twitter mood predicts the stock market," *Journal of computational science*, vol. 2, no. 1, pp. 1–8, 2011.

[40] B. W. Sanders, S. Bedrick, S. Broder-Fingert, S. A. Brown, J. K. Dolata, E. Fombonne, J. A. Reeder, L. A. Rivas Vazquez, P. Fuchu, Y. Morales, *et al.*, "Mobile and online consumer tools to screen for autism do not promote equity," *Autism*, vol. 27, no. 3, pp. 714–722, 2023.

[41] C. Pilton, S. Faily, and J. Henriksen-Bulmer, "Evaluating privacy-determining user privacy expectations on the web," *computers & security*, vol. 105, p. 102241, 2021.

[42] R. Abu-Salma, *Designing User-Centered Privacy-Enhancing Technologies*. PhD thesis, UCL (University College London), 2020.

[43] K. Seamons, “Privacy-enhancing technologies,” *Modern Socio-Technical Perspectives on Privacy*, p. 149, 2022.

[44] P. Chatterjee, R. Bose, S. Banerjee, and S. Roy, “Secured remote access of cloud-based learning management system (lms) using vpn,” in *Pattern Recognition and Data Analysis with Applications*, pp. 111–126, Springer, 2022.

[45] J. Longworth, “Vpn: From an obscure network to a widespread solution,” *Computer Fraud & Security*, vol. 2018, no. 4, pp. 14–15, 2018.

[46] J. W. Ross, P. Weill, and D. Robertson, *Enterprise architecture as strategy: Creating a foundation for business execution*. Harvard business press, 2006.

[47] G. Natriello, “The impact of evaluation processes on students,” in *School and classroom organization*, pp. 227–246, Routledge, 2013.

[48] D. Amo, P. Gómez, L. Hernández-Ibáñez, and D. Fonseca, “Educational warehouse: Modular, private and secure cloudable architecture system for educational data storage, analysis and access,” *Applied Sciences*, vol. 11, no. 2, p. 806, 2021.

[49] S. Kaur and G. Kaur, “Threat and vulnerability analysis of cloud platform: a user perspective,” in *2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 533–539, IEEE, 2021.

[50] V. Korhonen, “Future after openvpn and ipsec,” Master’s thesis, 2019.