e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

ENHANCING ANONYMITY DURING WEB BROWSING WITH TOR NETWORK

Chinmay Mirkute*1, Shraddha Gaikwad*2, Harita Virkar*3

*1,2,3M.Sc. Computer Science, B.K. Birla College Of Arts, Science & Commerce, Kalyan, India.

DOI : https://www.doi.org/10.56726/IRJMETS63817

ABSTRACT

The increasingly connected world that exists today creates dependence on public networks, both because more and more individuals are taking to the internet from cafes, airports, and other public places. Unfortunately, with this comes an enormous price: severe privacy and security threats. With data breaches occurring daily for millions of users worldwide, they reveal sensitive personal and financial information. Public networks typically involve more security risks. This is because low-level encryption and insecure connections allow malicious actors to intercept information, monitor user activity, and even collect access to personal user devices. The threats posed by such threats represent the clearest failure of the traditional security practices in terms of anonymity preservation. Despite efforts in cybersecurity, a perfect solution to secure anonymity remains elusive. While certainly some risks affiliated with existing tools can be somewhat mitigated, using VPNs, proxy servers, and even minimalist encryption protocols tends to often fall short of full security measures in ensuring one is, indeed, anonymous. Moreover, such tools frequently prove tricky to use, at least too expensive, or, quite simply, not good enough against increasingly sophisticated cyber threats. Another very important factor is the general public's poor education on best anonymity practices. Almost all users remain unaware of their vulnerability on public networks or which one of these methods would best protect their identities. Thus, most of the users unknowingly compromise their privacy, making it easy for the malevolent entities to track, intercept, and exploit their data.

This paper traces the historical development of anonymity enhancing technologies, unveiling key gaps in current approaches that have left users vulnerable to privacy invasions. We explore quite a range of widely available tools, including VPNs, proxy servers, and encrypted communications, to comprehend their strengths and weaknesses within the context of public network security. The analysis will also extend to more sophisticated anonymity frameworks, such as the TOR network that uses a decentralized relay system for hiding user identity, and emerging privacy-oriented technologies involving decentralized blockchain protocols and zero-knowledge proofs so as to introduce further obscurity in user data. TOR operates on a virtual encrypted tunnel that is used to transfer the user's data, enhancing the user's privacy policy and allowing the user to avoid being stalked by hackers. The dark web or TOR is sluggish because we normally need to use special browsers like TOR browsers, which do not connect directly with your computer to the dark web sites, or because your requests run via those three nodes, which use peer to- peer connections rather than core network connections. When you request a website and it shows on your screen, the delay between those stages increases. One of the main goals of this paper is to create propaganda in favor of anonymity of users in public networks by searching and analyzing applicable and functional means available on diverse devices and platforms. This paper discusses a broad range of tools and frameworks that enrich anonymity with the aim of equipping users with actionable insights into protecting online activities. Recommendations are made based on analyses of easing usability, accessibility, cost-effectiveness, and strength in resisting common cyber threats. In doing so, we propose best practices for users in the minimization of their digital footprint from interception or misuse on public networks. Therefore, this research bridges the gap between security solutions already in existence and the constantly increasing demand for online anonymity. It will devise effective strategies and spread awareness on anonymity techniques to contribute toward making the digital world a safer place. Our findings indicate that educating users in achieving effective privacy protections is important and call for greater initiatives to alert people into smart choices that enable them to make intelligent decisions in their digital security.

Keywords: Anonymity, TOR Network, Privacy, VPN, Proxy, Whonix, Layered Security.

I. INTRODUCTION

It's something of an open secret that many users have recourse to means such as the TOR 'onion' network in their pursuit of anonymity in light of the pervasive threat of intrusion in the virtual world. With this paper, we

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

look at ways of improving security by using layered anonymity techniques while browsing the web with specific emphasis on sustaining a VPN, a proxy, and Whonix in conjunction with the TOR network. We interrogate concerns regarding the performance and speed of the VPN only and proxy server and Whonix setups to find the best combination of layering tools for maximizing anonymity when accessing public networks without direct access to replications of the TOR-browser. From the analysis, it takes an interesting turn in the findings, to examine the climactic interplay between advanced features of privacy and usability-of what has come to be known as the usability controversy-as the layers to be synthesized into the optimal end user experience. Furthermore, the paper tries to make a global appraisal of security level that may be defined as quite promising.

The Tor protocol, beneficial for preserving civil liberties, appears highly profitable for various types of miscreants. The research presents a way to build a crawling mechanism by extracting onion URLs from malicious executables. Using machine learning, we were able to classify the Tor-using malware with an accuracy rate of 91%. The anonymity of evaluation nodes is assessed based on stable intervals and behavior baselines defined according to their normal operating status. The anonymity of the network is evaluated using an improved normalized information entropy method that refines anonymity evaluation to the anonymity of each node. Our approach utilizes dynamically changing network anonymity based on multiple anonymous attributes and better reflects the degree of anonymity in anonymous systems. The Tor anonymity network is one of the most popular and widely used tools to protect the privacy of online users. Traffic analysis is a very strong tool that can be used for internet surveillance. This report addresses the issue of detecting intruders from hiding behind privacy-protecting anonymity networks. A growing concern is the use of anonymous proxy services, as recent security breaches reveal the use of SSH and HTTPS by malicious users. We evaluate our approaches with SSH and HTTPS connections, showing high performance for both applications.

II. LITERATURE REVIEW

TOR (The Onion Router) Network, known for providing anonymity, is one of the most used applications for privacy protection. This makes sense considering the fact that TOR achieves this objective by directing traffic through several volunteer relays which mask out the user IP making it hard for any other parties to monitor activities on the web. But while users can count on the TOR for anonymity a significant number often complain about the slower speed of browsing and issues of latencies. These performance problems have encouraged more investigation into the TOR tool and how it can be used together with privacy protection mechanisms like VPN (Virtual Private Network), proxy, and Whonix to increase user security.

Unlike a standard web browser, Tor garners its authority through the third-party voluntary structure that it utilizes, which makes the network one of the most universal applications to ensure privacy compliant operations. Nonetheless, TOR is effective, but it has an unresolved issue with regards to performance, especially considering the element of latency. This has resulted in a closer examination of how TOR can be used alongside other privacy security technologies to overcome these constraints without compromising security. In this respect, it is important to evaluate anonymity and performance in order to determine the balance between security and usability that might be required when using TOR with VPNs, proxies, and Whonix.

1. Traffic Analysis and Its Associated Security Weaknesses

TOR can assist in privacy protection however it is not immune to traffic analysis. These attacks pose a serious risk to the network security since they permit an opponent to observe and scrutinize the network traffic with the aim to determine some patterns and, in the process, possibly pinpoint the users. As more people utilize TOR with various other tools, this inadequacy has resulted in a growing demand for better privacy. Traffic analysis remains the most efficient method for internet surveillance, and its impact on the privacy of TOR users has been well-established, warranting the need for additional measures of protection.

2. Using VPNs, Proxies and Whonix Alongside TOR

Users are faced with the challenge of exploiting the strengths of TOR while seeking to counter the threats of traffic analysis, thus many users incorporate other resources such as VPNs and proxies to TOR. VPNs act as an additional layer of encryption so that the users data is protected before entering the TOR network helping to avert any traffic analysis that might take place outside the TOR network. Proxies make anonymity even better by allowing the users traffic to pass through intermediary servers. The results of these studies indicate that

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

employing TOR as well as VPNs and Proxies was beneficial in protecting a user's privacy –however, there was a tradeoff in the performance of the user. This was enhanced with the addition of Whonix which is an OS designed specifically for anonymous security.

3. Whonix: Security in Whonix During Isolation Mode

Whonix is an innovative operating system designed with privacy in mind and is divided into two segments: Whonix-Gateway that acts as the bridge with the TOR network and Whonix-Workstation that sends its traffic to TOR. This division of roles guarantees that the user's traffic is sent over the TOR network at all times providing an extra level of safety. Some of the weaknesses found in other setups are also compensated by Whonix, not least due to the segregation of the user's environment and the lower potential of data leakage. Whonix is a part of the solution to maintain a high level of internet privacy along with VPNs and proxies, however, like any other security tool it comes with browsing speed trade off.

4. Layered Security and Usability Difficulties

One of the key problems when TOR is used with VPNs or proxies in conjunction with Whonix, is the reduction in usability. Of course the introduction of several protective layers makes it slow to continue browsing and makes the task complicated for the user. This exchange of usability for privacy is referred to as the "usability controversy". Constructing users' privacy was always a focal point, therefore the increased security features should never be so significant that ordinary user experience becomes affected. The focus here should be how to maximise anonymity without compromising the effectiveness and simplicity of user navigation on the internet.

5. Exploiting Anonymity through Throughput Networks

While there are networks like TOR which users protect the privacy with, these kinds of networks also have some visually adverse purposes. As of late, breaches have been associated with the use of TOR together with anonymous proxy services. According to reports, such malicious users have, for instance, employed TOR in their hacking and fraudulent activities. It also points out the necessity of employing suitable detection mechanisms of the malicious users without violating the privacy of legitimate individuals. This is, however, one of the key factors that need to be addressed in order to improve security and trust of anonymity networks in the first place.

III. METHODOLOGY

The main goal of this study is to evaluate and compare performance and security of the layered anonymity measures, comprising a VPN, a proxy, and a Whonix together with the TOR network. The methodology involves a number of distinct stages to facilitate in-depth analysis, from data collection to assessment of performance. What follows is a comprehensive and detailed description of the methodology that was adopted in pursuit of the research objectives.

1. Sources of Data

The data for this study was collected by performing the primary and the secondary data collections from the trusted academic databases. The experiments had been carried out with the use of network monitoring tools in order to determine the performance and the anonymity of the different configurations of VPN, Proxy, and Whonix.

- Primary Data Sources: The primary data was collected through several sessions of controlled browsing experiments and examining the relevant variables such as setup and the parameters of the tests conducted (speed and latency).
- VPN Server: A VPN provider of the experiment is located in different geographical zones.
- Proxy Server: Proxy service was utilized through manually inserting the IP addresses and ports.
- Whonix Configuration: Whonix was configured on a virtual machine in VirtualBox to remain in different environments during the experiments.
- Secondary Data Sources: Other authors' works, scientific articles, dissertations, reviews on the subject of the study plus heretofore results of effectiveness of VPNs, proxies, and Whonix in enhancing TOR's anonymity and security were used for comparative analysis.

2. Experimental Setup and Configuration

It was aimed to establish the experimental setup in order to assess the individual effect of VPN, Proxy and

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

Whonix on both performance and anonymity. The configuration steps are as follows:

- VPN Setup: The VPN software was set up on the host and linked to one server.
- Traffic Routing: All traffic from the host machine was routed through VPN and its performance monitored using network monitoring tools.
- Evaluation: The VPN connection was checked as how well it could protect the user's IP address and evaluated the effect on browsing speed and latency.
- Proxy Setup: Installation of a proxy server (using a proxy tool) on the host machine.
- Traffic Routing: The traffic was routed first through the proxy. Network performance is assessed, while the changes IPs are recorded.
- Evaluation: The effect of proxy setup on anonymity was watched together with the performance which included fluctuations in the IP and speed of connection.
- Whonix Setup: Whonix was installed on VirtualBox as a guest OS with two components: Whonix-Gateway and Whonix-Workstation; both were set up to send traffic via TOR.
- Layered Routing: The routing of traffic from the virtualized Whonix environment is done through the TOR (by Means of Whonix).
- Evaluation: This final step consisted of a monitoring and comparing the performance (speed and latency) and anonymity (IP masking, traffic analysis resistance) of this multi-layered configuration.

3. Measuring Performance and Anonymity

In order to assess the performance (speed, latency) and the effectiveness in preserving anonymity (change of IPs, traffic analysis), the following instruments were employed.

- Speedtest.net: A speed test tool which helps to know the download or upload speed, and the latency for each configuration. This was necessary in the respect of determining how each configuration affected the performance of the browsing activity.
- IP Checkers (WhatIsMyIP.com, ipleak.net): These sites assisted the researchers to determine the change of IP addresses when contrasting different privacy settings on the configurations to ensure that the addresses were effective in obscuring the user's real IP.

4. Data Collection and Analysis

The data that was gathered from the experiments has been placed in order and evaluated as follows:

- Performance Metrics: In the case of each setup data was captured during several run-ups about connection speed, download, upload rates and latency.
- Anonymity Metrics: The level of anonymity was first given an estimate by the number of unique IP's changed during the process. Any risk of data leakage including DNS leaks was reported.
- Usability Concerns: User experiences while navigating in any of the platforms were also captured in terms of page loading speed, response time and other factors that will be useful in determining whether there are any trade-offs between security and usability.

5. Ethical Considerations

This research relates to privacy and security tools and thus ethical issues are crucial. Not even a single illegal activity or unethical browsing was performed during the testing phase. Any tools and techniques that were used were within the terms and conditions and policy of the tools that were used in the research. Further, the research refrained from testing exit node vulnerabilities due to privacy issues.

IV. IMPLEMENTATION AND ANALYSIS

Throughout the research, the tools and technologies listed below were employed:

1. **VPN**
2. **PROXY SERVER**
3. **WHONIX**

Although VPNs work by covering a user's IP address with a VPN server's IP in order to enhance a user's privacy, this comes at the cost of increased latency and a dropped speed due to some encryption overhead as well as

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

slight issues with DNS leaks. On the other hand, Proxy Server circumvents a user's IP address by routing it through the IP of a proxy server, which is known to add relatively high latency and considerably lower speeds especially in the case of free proxies. Irrespective of been able to offer a moderate privacy protection, it possesses security threats such as man-in-the-middle attacks. Lastly, Whonix (TOR Network) connects a client's traffic via the TOR network and is able to fully disguise a user's IP address; thus making the tracing of his location very difficult. The tradeoff here is that it also has very high latencies and slow speeds which makes it very effective for secure browsing and confidential transactions but not for tasks that require a lot of bandwidth.

1. VPN:

Implementation: To implement the VPN-only option, one can start by choosing a suitable VPN provider (for instance, Proton VPN) that has desirable security, speed and privacy features. Then, install this VPN software on your computer or a device used for the purpose. At this moment the application is installed on your device, sign in and select the server to connect to. Once the VPN connection has been established, you can go to an IP-checking site such as whatismyip.com to ascertain if your own IP has been replaced by that of the VPN server.

Then, for performance impacts, other tools like Speedtest.net can be used to assess ping, download as well as upload speeds. The tests are carried under various locations of the VPNs so as to see the impact of geographical distance on performance.

Figure 1: Proton VPN

Analysis

- Privacy: VPN's privacy feature is the original IP of the user as it will be hidden by the IP of the VPN server making it impossible for the websites to trace back to the person being VPNed. However, DNS leaks may sometimes occur so DNS leak protection is provided in the VPN settings, and should be activated.
- Performance: The VPN setup will have moderate latency due to encrypted and rerouted traffic through the VPN server. Speed degradation can be expected when you're using server locations that are the furthermost points in connection to your physical locations.
- Usability Notes: VPNs have numerous benefits for the purpose of anonymous surfing and secure connections on wi-fi networks. Yet, depending on the overhead compression options, the destination page may load slower than it is necessary or there will be problems with DNS addresses if the VPN is not configured properly.

2. Proxy Server:

Implementation: To configure the proxy settings, decide on a proxy provider or set one up on your local machine. For instance, on windows, one would go to Settings – Network & internet- Proxy settings and enter the service's proxy IP and port number. A manual proxy could be configured as well by using third party tools/software. Once established, check the setup by using proxy servers to access sites such as whatismyip.com and establish whether the external IP addresses are the same. For testing performance, use Wireshark or Fiddler for network traffic capture & analytics. Carry out a speed test where ping, the downloading speed and the uploading speed is assessed and checks for any detectable latency change on the network.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

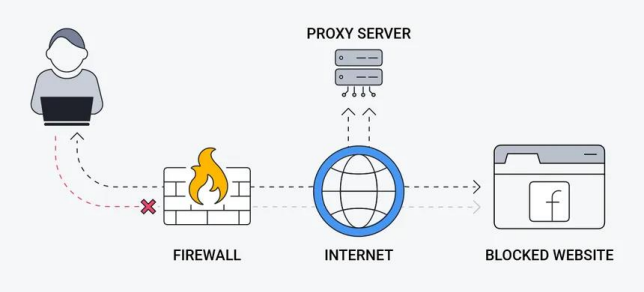

Figure 2: Proxy Server

Analysis

- Privacy: The user's actual IP is concealed by the proxy server that then forwards the traffic through its own IP, ensuring a fundamental level of anonymity to a primitive extent. Remember that since proxies are more exposed especially free or police proxy, they are subject to more attacks.
- Performance: Proxy servers have more delay than VPN; a typical example is when free servers that are heavily burdened or far from the user are used. The speed tends to deteriorate with the distance as well as the proxy's capacity and the proxy type, which can be HTTP, SOCKS, etc.
- Usability Notes: Proxies are widely employed for IP theft though they can be realized with performance and security concerns. Free proxies are usually slow and may not even provide encrypted traffic which makes them inappropriate for sensitive sites.

3. Whonix (TOR Network):

To use Whonix, it is necessary to install Whonix-Gateway and Whonix-Workstation in a VirtualBox environment. It is Whonix-Gateway who facilitates the connection by routing all the traffic through TOR network while Whonix-Workstation is where all the applications, such as the browsers, are hosted. While the virtual machines are prepared, remember to launch Whonix-Gateway first in order to establish a connection with TOR, and afterward launch Whonix-Workstation. Make sure that Whonix-Workstation has been set in a way that all it's internet traffic is routed via Whonix-Gateway.

As soon as the Whonix system is complete and operational, take an IP check via whatismyip.com to check that indeed the external IP is concealed behind the TOR exit node. Also, run check on Speedtest. net to confirm the ping, download as well as upload while browsing. Further, check the Activity through Wireshark with the compression of the network flow.

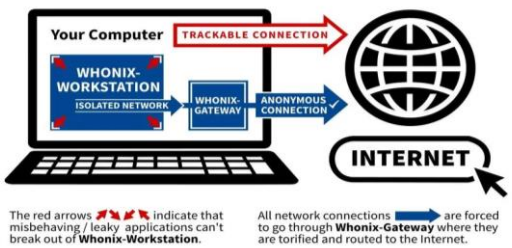

Figure 3: Whonix

Analysis

- Privacy: Whonix, which works together with the TOR network, provides the most reprieve in terms of anonymity since it hides your IP address as well as circulates the network traffic through various TOR relays. It is practically impossible to identify the initial user because of the use of several layers of encryption and routing.
- Performance: Because of the presence of several decentralized TOR layers, the amount of latency is much greater when compared to other VPNs and proxies. The download and upload speeds are generally quite low making Whonix inappropriate for downloading or streaming due to the high bandwidth requirements. Also, the use of onion routing for TOR cause high latency time.
- Usability Notes: Who is Whonix best for? It is perfect for secure and anonymized web usage. Whonix has been specifically optimized for certain tasks where privacy is of utmost importance such as retrieving

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

sensitive information, bypassing censorship efforts, or transmitting messages securely. Yet, because of its lack of speed, the use of whonix would be inappropriate when engaging in activities such as gaming, fast web surfing or videos online.

It appears from the performance constraints mentioned, users have the option of internet connectivity but like any other person who regularly uses TOR Network which enhances security through concealment of traffic, certain delays are detected which might be unfavorable. Hence, it is important to prioritize security requirements while still being able to browse freely and securely."

V. RESULTS

VPN: With a VPN, a real IP is concealed within a server's IP with added latency while speed performance goes low due to encryption. The level of privacy offered is good but DNS leaks can be encountered once in a while. It does not provide against ID theft but is suitable for most browsing activities though high bandwidth tend to be affected for example streaming.

Proxy Server: Just like VPN, a proxy hides the user's IP address with that of the proxy server. Proxy does not provide traffic encryption and hence lacks on protection from third-party interception. Security is reasonable but predisposed to man-in-the-middle scenarios for such proxies that are untrusted. Proxies tend to slightly increase latency and slow down speeds especially free ones which might not serve high-security instructions well.

Whonix (TOR Network): Whonix sends its traffic across the TOR network thus enhancing user's security by ensuring that the user engages in multiple layers of encryption. Its anonymity levels are higher than that offered by VPNs or proxies but very slow speeds and high latency makes Whonix unsuitable for time sensitive activities such as gaming or streaming. Whonix is ideal for browsing and secure tasks that don't rely on speed but security instead.

Table 1. Comparative Analysis:

VPN	PROXY SERVER	WHONIX
VPN is a quite efficient tool in balancing between privacy and performance metric, however, depending on where the user is located, bandwidth may be affected. It is appropriate for average usage of the web, protecting Internet communications, and operating in a certain degree of non-disclosure without emphasizing speed.	Proxy Server enables its users to disguise their IP addresses; however, this method is not suitable in most cases for usage as a secure identity shift because of possible breaches and effectiveness drop (particularly in case of free proxy usage) and hence goes without much emphasis in the work. A user can use them for browsing the internet though without making it a priority.	Whonix offers, perhaps, the best protection and anonymity; however, the price to pay here is the speed and high latency unpredictability. It's great for use in tasks where one has to maintain most supreme privacy, however, in cases where one has to browse normally or use high bandwidth it is not the best option.

Table 2. Summary of Findings:

The subsequent observations were made during the practical implementation:

Configuration	IP Address	Ping(ms)	Download Speed (Mbps)	Upload Speed (Mbps)	Usability Notes
VPN	VPN IP	Moderate	2.30 Mbps	20.30Mbps	Good privacy protection, but reduces the speed moderately and increases the latency only a usual amount. Rare DNS leaks.
Proxy Server	Proxy IP	Higher	6.58 Mbps	5.15 Mbps	IP is masked with proxy, but latency increase and speed drop considerably.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

					There are security threats using free proxies.
Whonix	TOR Exit Node	Very High	1.33 Mbps	0.00 Mbps	Highest level of privacy, but the speed is very low and the latency is quite high. Preferred for secure browsing only.

Results:

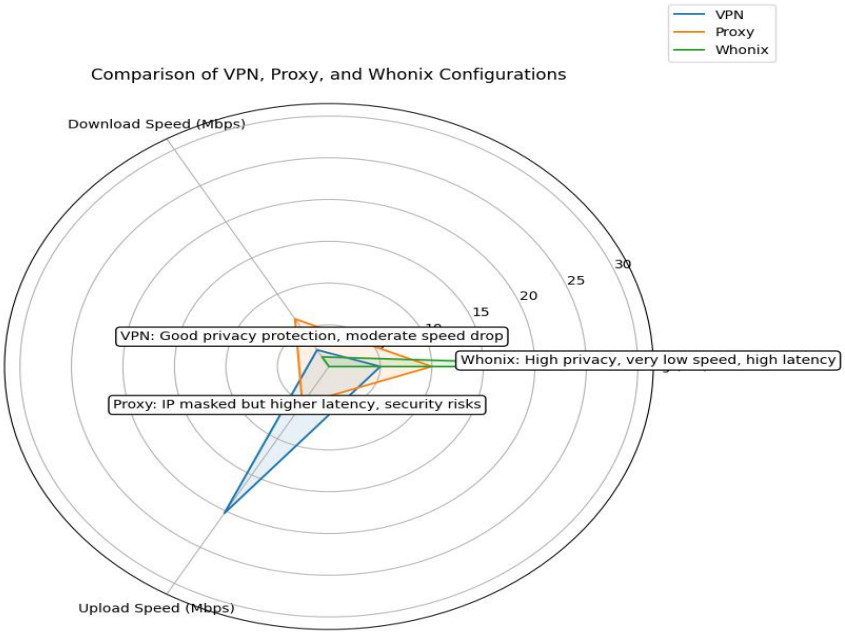

Figure 4: Comparison of VPN, Proxy, and Whonix Configurations

VI. CONCLUSION

This study focuses on the effectiveness of layered anonymity techniques including VPN, proxy server, and Whonix (TOR network) in improving data protection and privacy during web browsing, especially through public access. The aim was to evaluate the extent to which these tools, when used synthetically, affect the level of anonymity and shape the parameters of speed and usability of the online environment, allowing the use of the TOR browser only in indirect form, as an example of the tools which are usually attributed to the protection of privacy.

During examinations of this research, we attempted to individualize the assessment of VPN, proxy servers, and Whonix tools in isolation or in combination. Each tool provided some security and anonymity, but each had its own benefits as well as drawbacks. The use of a VPN on its own provides good IP masking of the user and adds encryption to the connection. It is decent in terms of privacy, but the added latency and occasional DNS leaks make it less useful when high speed is required. Nevertheless, VPNs stay one of the most robust solutions for privacy protection on the internet as they prevent unwanted exposure in the most needed conditions. In terms of privacy, the proxy server does help users mask their IP addresses. However, they lack encryption which exposes users to several weaknesses such as MITM (man in the middle) attacks. The void of encryption along with add barriers

Whonix software provides the most enhanced anonymity since it is connected via the TOR network that performs numerous hopping and makes traffic analysis very difficult. But with this extra security the performance is unfavorably affected. Because of the high latency and low download speeds, using Whonix is not appropriate for video streaming and gaming applications. Even so, Whonix is very good for privacy a users as it uses anonymizing technologies that are aimed at obscuring the users location and activity reach.

The use of VPN together with a Proxy and Whonix combines the best of these features in providing the highest degree of anonymity and security. It is possible to use all these tools at once to obtain combinations of benefits – the encryption of the VPN, the IP of the proxy, and the Whonix's multi-layered TOR encryption, which is safe

while Internet surfing. The downside is that the combined use of all 3 features is bound to significantly affect the level of performance. Increase in latency and decrease in browsing speed demonstrate the use providers amenities and security features comes at a cost.

In this regard, it has become apparent that although the scraping of layered anonymity becomes a potent weapon for masking one's identity, it lowers the efficiency. Users who need the highest level of security and privacy will find the solution quite efficient but slower.

VII. REFERENCES

[1] "Achieving Anonymity with the helpof TOR (TOR A Review)."

[2] D. S. Kolavennu, M. Gilda, S. Asif, and T. P. Tejaswini, "Unveiling The Malicious Users Behind the Anonymity Networks," vol. 11, no. 1, 2024.

[3] J. Cui, C. Huang, H. Meng, and R. Wei, "Tor network anonymity evaluation based on node anonymity," Cybersecurity, vol. 6, no. 1, p. 55, Nov. 2023, doi: 10.1186/s42400-023-00191-8.

[4] A. Buitrago López, J. Pastor-Galindo, and F. Gómez Mármol, "Updated exploration of the Tor network: advertising, availability and protocols of onion services," Wirel. Netw., Feb. 2024, doi: 10.1007/s11276-024-03679-4.

[5] J. Bergman and O. B. Popov, "Recognition of tor malware and onion services," J. Comput. Virol. Hacking Tech., vol. 20, no. 2, pp. 261–275, Apr. 2023, doi: 10.1007/s11416-023-00476-z.

[6] Y. J. S. Batunanggar, A. Widjajarto, and M. T. Kurniawan, "Implementation and Analysis of Profiling Mechanism for Anonymity and Privacy on Whonix Operating System," vol. 6, no. 1, 2024.

[7] M. AlSabah and I. Goldberg, "Performance and Security Improvements for Tor: A Survey".