Unmasking the True Identity: Revealing the Real IP Addresses Concealed by VPNs/Proxies

Jatin Aggrawal
School of Computing
Science and Engineering
VIT Bhopal University
MP 466001, India
jatin.aggrawal2021@vitbhopal.ac.in

Arpit Sivakumar
School of Computing
Science and Engineering
VIT Bhopal University
MP 466001, India
arpit.sivakumar2021@vitbhopal.ac.in

Lalit Sahu
School of Computing
Science and Engineering
VIT Bhopal University
MP 466001, India
lalit.sahu2021@vitbhopal.ac.in

Muskaan Bhotika
School of Computing
Science and Engineering
VIT Bhopal University
MP 466001, India
muskaan.bhotika2021@vitbhopal.ac.in

Vikas Kumar Jain
School of Computing
Science and Engineering
VIT Bhopal University
MP 466001, India
vikaskumar@vitbhopal.ac.in

***Abstract*—After thorough familiarization with currently existing research work progresses under the same constraint posed by the real-world problem of easy access to the anonymity that illegal and unethical threat actors obtain by the use of Virtual Private Networks or VPNs, it was understood that there exists high significance in devising a solution for the same. Protection under VPN could be misused, that is, used for practices that may involve unlawful intention(s). The authors provide a novel methodology for preventing attacks by identifying the threat's IP address while shielded by a VPN. The method utilizes underlying patterns in the traffic generated by threat actors to correlate their VPN-assigned IP addresses with their real identities. Upon identification, appropriate countermeasures can be applied to neutralize the risks posed by these threats. The key innovation lies in leveraging traffic characteristics that remain identifiable even under VPN encryption. Preliminary results indicate the feasibility of the approach. When successfully developed, the technique has the potential to improve network security by allowing the identification and mitigation of threats hiding behind VPN anonymity.**

***Index Terms*—DNS, Honeyfile, Honeypot, IDS/IPS, IP Address, Network Security, WebRTC.**

I. Introduction

Crackers, Script Kiddies, Hacktivists, and whatnot, are taking over this digital age by storm. And the mass is unarmed. The most profound pillar of support they obtain in order to get a multitude of malicious functions executed, is 'Anonymity'. Going by the traditional definition, it can be defined as "situations where the acting person's identity is unknown". Interestingly, corresponding to this work of research, the authors aim to seek a feasible, efficient, and coherent resolution to this threat, aiding the culture of proactive and defensive caliber under the sphere of Cyber Security.

A Virtual Private Network (VPN) is a private and secure communication tunnel that enables users to connect to the internet or a private network from any possible distance while maintaining the security and confidentiality of their data. In essence, VPN makes it seem as though the user's device is directly linked to the private network by extending the functionality of a private network across a public network, like the Internet.

A VPN's primary purpose is to encrypt all data sent between a user's device and the VPN server. Data is converted into a secure code through encryption, which prevents information from being intercepted and decoded by unauthorized parties. In addition to protecting private information like login credentials, financial information, or private messages, this method also stops internet service providers (ISPs) and governmental organizations from watching online activity.

There are various VPN configurations, including site-to-site and remote access VPNs. Data encryption is just one advantage of VPNs. Bypassing geo-restrictions is a benchmarking attribute. Although VPNs provide strong privacy and security safeguards, picking a reliable VPN provider is crucial. The aim of utilizing a VPN may be defeated by some unreliable or free VPN providers that collect user data or undermine security.

VPN is an effective tool that gives users more freedom, privacy, and security when accessing the internet or private networks. VPNs have developed into a crucial tool in the contemporary digital environment by encrypting data and directing traffic over secure channels. To maximize the benefits while protecting their sensitive information, users should take care while choosing reputable providers.

The structurization of this paper ensures a thorough flow of comprehension. Commonly used techniques subsection dwells on other parallelly used methodologies and explanations for

the same. Comparison of VPNs represents a clear comparison of various available options catering to a variety of needs, owing to the diversity of user base in need of this technology with varied requirements as well. Over the years, how this real-life problem statement influenced the netizens are made clear with the aid of statistics by the Relevance of Study. Proposed Work illustrates the research work projectile of how the authors aim for the proposed methodology to be implemented and executed. Implementation Analysis is one of the final phases where post-execution of the work is reevaluated. Here, the authors also propose the Future Work direction, shedding insight on how this research area can be developed and improved. The finale of this work of research is marked by the conclusion, putting all the information gathered, comprehended, interpreted, worked on, implemented, and analyzed into a nutshell.

II. Background and Related Works

A. Related Works

Various techniques have been proposed by researchers to trace the real IP addresses behind VPNs and proxies.

- Nithesh Aravind et al. (2023) analyzed several approaches for identifying the origin IP address when a connection is made through an anonymizing network. They found that traffic analysis attacks based on timings, packet sizes, and protocol analysis can help reveal the real IP with varying degrees of accuracy. [7]
- Fan (2019) proposed a method based on the clustering of TCP profiles to identify VPN users. They showed that VPN users tend to have distinct TCP characteristics compared to normal Internet users, and their clustering approach could detect VPN users with high accuracy. However, this method requires a large amount of network traffic data for training. [3]
- Zainu al. (2019) developed a trace-back algorithm based on HTTP header fields. They found that several header fields, like Accept-Language, User-Agent, and Cookie, can reveal identifying information that helps link traffic to original IP addresses. They implemented a prototype system that could trace real source IPs with over 80 percent accuracy. [11]
- Dai et al. (2019) introduced a trace-back method based on website element fingerprinting. They showed that the rendering of web elements like images, texts, and ad elements can serve as fingerprints that remain unique for a given IP address, even behind VPNs. Their experiment on Alexa's top 500 websites achieved 74 percent accuracy in identifying real source IPs. [1]
- IPSec proven to be the most secure VPN protocol possesses setbacks of its own. Managing and configuring may appear to be challenging. Although Layer 2 Tunnelling Protocol (L2TP) is a less secure VPN protocol than IPSec, it is more user-friendly. The least secure VPN technology is Point-to-Point Tunnelling Protocol (PPTP), but it is also the most straightforward to set up and maintain. The phion VPN system was straightforward to use and configure. The phion VPN solution was not, according to the research, as scalable as some other VPN solutions. The study discovered that IPSec is the ideal option for businesses in need of a highly secure VPN service. L2TP and PPTP, however, are also good choices for companies that don't require the utmost level of security. [2]
- This study has its focus point in enabling encryption at a more practically resourceful level, aiding VPN security to be a more preferred channel of choice for individuals, organizations, and businesses. For this, the methodology chosen is multi-phase encryption. This selection is made post-analysis of the edge that this encryption capability holds over traditional ones. This also ensures to be in sync with the currently existing basic functioning of VPN with a blend of the contemporaneity of encryption of payload for higher performance in terms of security. The point of barrier caused by this ideation is the computation requirements, a vital factor for the smooth working of the proposed work. [10]
- The analysis suggests that a large number of VPN clients do not offer robust security features like perfect forward secrecy (PFS). Even if an attacker manages to penetrate the VPN server, PFS is a cryptographic technique that makes it challenging for them to decrypt previously encrypted communications. Leakage of IPv6: The study discovered that 12 out of 15 evaluated commercial VPN clients leaked the VPN user's IPv6 address. This is a severe security flaw since it enables attackers to monitor a user's online behavior even while the VPN is using encryption. 4 out of 15 commercial VPN clients were discovered by the study to be vulnerable to DNS hijacking. Attackers may take advantage of this flaw to reroute VPN users' DNS requests to harmful websites. According to statistics, only 3 out of 15 commercial VPN clients had PFS or other robust security measures. As a result, users of the other 12 VPN clients run the danger of having past communications intercepted and decrypted by hackers. [8]
- The authors describe how to utilise deep packet inspection (DPI) to identify VPN tunnels and identify the user's identity and location by examining VPN data.the use of data analysis and mining techniques to identify patterns in network traffic that can be exploited to locate the source of Tor communication. Additionally, IP geo-location may be employed in order to obtain the location of the Tor service. The VPN client, the personal computer corresponding to that particular node may install a virtual NIC (network interface card) while there exists the physical NIC. To accomplish this, you must ask users who access the webserver to run the script that checks the origin IP. It determines if you are using a VPN or not. If you're using a VPN, the original NIC IP (original IP) and the IP (VPN Entry) of the virtual NIC are given to the web server, which then retrieves the script that was executed.

[9]

- This study focuses on resolving the setback that the simplicity of Internet Protocol holds which is the lack of detection of authenticity at packet level. This widens the potential for major threats such as DDOS. The proposed methodology is the use of passive detection and analysis of spoofed traffic. The methodology commences with the detection of Packets with Stray source IP addresses, which are generated due to misconfiguration and carry no malicious intent. This is followed by, packets with a spoofed source IP address. This complies with the function of misinterpreting the source IP address. The distinguishing stage of both these categories is a highly crucial phase. The size and completeness of the BGP-derived address spaces of each AS are carefully examined here, in order to achieve this. [5]

B. Commonly Used Techniques to Get IP Addresses

The realm of uncovering hidden IP addresses behind VPNs and proxies involves a diverse array of techniques, each varying in effectiveness and output generation. The exploration of these methods provides valuable insights into the challenges faced by cybersecurity experts striving to trace and counteract cyber threats. Here are several notable techniques employed by malicious actors:

1. IP Address Correlation: This technique involves observing and analyzing network traffic and behavioral patterns. By comparing an individual's behavior while connected to a VPN and when not connected, it becomes possible to deduce patterns that might lead to the discovery of their actual IP address. Subtle differences in browsing habits or communication patterns can provide hints about the user's real identity.

2. DNS Leaks: Sometimes, a user's device may unintentionally leak Domain Name System (DNS) requests outside the protective VPN tunnel. This leakage can expose the user's true IP address, as the DNS requests are routed through the user's default DNS servers rather than the VPN's servers.

3. WebRTC Leaks: Web Real-Time Communication (WebRTC) technology enables browser-based communication. However, it has the potential to inadvertently reveal a user's genuine IP address, even when a VPN is active. This vulnerability arises due to the browser's direct communication capabilities.

4. Browser Fingerprinting: Even when a VPN is utilized, web browsers can inadvertently leak information about a user's system configuration. This information can be utilized to create a unique "fingerprint" that identifies the user's device across different browsing sessions, potentially revealing the real IP address.

5. Social Engineering and Phishing: Cybercriminals often resort to social engineering tactics or phishing attempts to manipulate individuals into disclosing their actual IP addresses willingly. Through deceitful means, attackers can gather information from users that aid in identifying their real identities.

6. Metadata Analysis: Examining metadata associated with online activities, such as timestamps, session durations, or usage patterns, can provide valuable insights for user identification. By analyzing patterns of behavior and online presence, cybersecurity experts may piece together clues that lead to the identification of a user's true IP address.

7. Traffic Analysis: Advanced traffic analysis techniques involve scrutinizing network traffic patterns to identify trends and anomalies. These methods can help experts locate users by deciphering unique patterns associated with their online behavior, ultimately leading to the revelation of their real IP addresses.

C. Evolution of VPNs

Virtual Private Networks (VPNs) have evolved significantly since the 1990s when they first appeared on the scene. Here is a succinct summary of its development:

(i) Early VPNs: In the beginning, VPNs were mainly used to link distant offices and enable secure internet communication. They typically used leased lines to create private connections between scattered locations and were hardware based. Early VPNs prioritized data privacy and encryption to safeguard sensitive information while in transit.

(ii) PPTP and L2F: To enable secure internet connection, Point-to-Point Tunnelling Protocol (PPTP) and Layer 2 Forwarding (L2F) became well-liked protocols in the late 1990s. L2F was created by Cisco, whereas PPTP was created by Microsoft. These protocols expanded the use of VPNs outside of corporate settings by enabling users to create secure connections to their corporate networks over the internet.

(iii) IPSec: In the early 2000s, Internet Protocol Security (IPSec) became a widely used standard. As it operated at the network layer of the OSI model, it provided a more reliable and secure solution for VPNs. In order to ensure secure communication between two endpoints over an untrusted network like the internet, IPSec provided encryption, authentication, and integrity checking for data packets.

(iv) SSL/TLS VPNs: SSL (Secure Sockets Layer) and its descendant TLS (Transport Layer Security) VPNs became more and more popular as remote work and the necessity for safe access from untrusted networks grew. SSL/TLS VPNs could be accessed using common web browsers, making them more user-friendly and generally available than conventional VPNs that needed specialized software.

(v) Mobile VPNs: As smartphones and other mobile devices proliferated, so did the need for secure access while on the go. Mobile VPNs were created to offer safe connectivity for users on the go, enabling them to connect to public Wi-Fi networks

and use encrypted tunnels to access corporate resources and the internet.

(vi) VPNs based on the cloud: VPNs were no exception to how cloud technology revolutionized company operations. With the advent of cloud-based VPN solutions, businesses may now set up and control VPN connections using cloud service providers. Compared to conventional on-premises VPN systems, this strategy offered scalability, flexibility, and lower infrastructure expenses

D. Relevance of study

Most notable Cybercrimes that were unsolved due to lack of determination of the culprit's IP address.

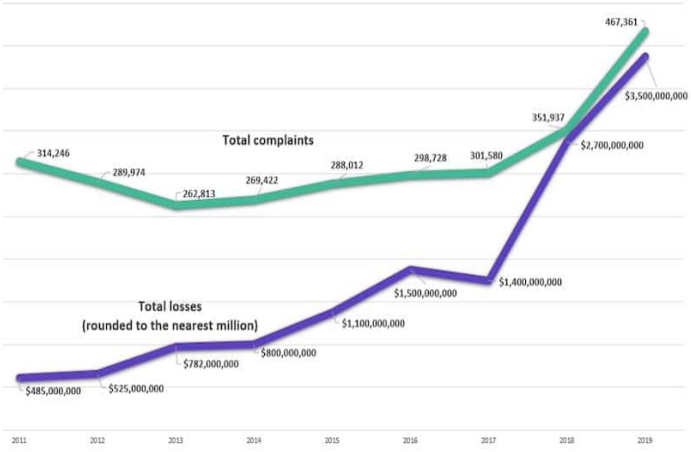

Fig. 1. Statistics.

The diagram shows the number of total loans and total complaints for two types of cybercrimes: those that were unsolved due to a lack of determination of the culprit's IP address, and those that were solved. The data is from the FBI IC3 2019 report.

The graph shows that there were a significant number of cybercrimes that were unsolved due to a lack of determination of the culprit's IP address. In particular, there were 467,361 total loans and 209,422 total complaints for these unsolved crimes. This represents a significant financial and emotional cost to victims.

The graph also shows that VPN-enabled protection was a major contributor to unsolved crimes. In particular, 5485,000,0000 loans were made and 787,000,000 US Dollars in losses were reported for crimes that used VPN-enabled protection. This suggests that cybercriminals are increasingly using VPNs to hide their IP addresses and make it more difficult for law enforcement to track them down.

The diagram highlights the importance of being able to determine the culprit's IP address in order to solve cybercrimes. IP addresses are a valuable tool for law enforcement, as they can be used to track down cyber criminals and bring them to justice. However, cyber criminals are increasingly using VPNs and other tools to hide their IP addresses, making it more difficult for law enforcement to solve these crimes.

NOTE*: It is important to note that VPN-enabled protection is not the only modus operandi used by cybercriminals. However, it is a major contributor to unsolved cybercrimes. Law enforcement agencies need to develop new tools and techniques to combat the use of VPNs and other anonymization tools by cybercriminals.

III. Proposed Work

A. Techniques

Honeypot: A honeypot is made to seem exactly like a real computer system, loaded with real-looking software and data, to fool fraudsters into believing it's a legitimate target. It is not a remedy developed to address a particular issue. Instead, it acts as a tool for information that may help you identify present hazards to your company and spot emerging ones.

B. Proposed system

To determine the true IP address of any unauthorized users who access your network using a proxy or VPN. By developing a honeypot security method, it is possible. That unauthorized users could join. In this way, we may entice the attacker, and when he tries to take our fraud data, we can send our payload along with it. The real IP address, data, logs, and files of the attacker's system will be sent when our payload successfully reaches the attacker's system.

Select a platform that is appropriate: There are various platforms that can host websites, including BlueHost, Hostinger, and HostGator, among others. Pick a platform that works for your needs and skill set.

Establish teh honeypot: After deciding on a platform, it is necessary to set up the honeypot file or honeyfile. It could contain false goods, pictures, and descriptions, but make sure they appear authentic and polished.

Install security measures: Since the honeypot is designed to draw attackers, it needs to be protected with security measures to prevent actual customers from coming onto it by accident.

Keep your eyes on the honeypot: Once the honeypot has been installed, it must be carefully watched for intruders. Several tools, including web application firewalls, intrusion detection systems, and log analysis tools, can be used for this.

Analyzing the data: Examining the information gathered from the honeypot to learn more about the strategies and methods employed by attackers. This can aid in the creation of improved security protocols and a general increase in the safety of websites.

IV. Result and Analysis

A. Implementation

To trace the actual/real IP address of the unauthorized user who accesses via the VPN server or proxy servers to prevent an attack. The proposed work was implemented by employing the subsequent strategy to stop the attack:

1. Platform: For the platform, our local machine is used as a web server.The website is a demo website using a local server in this case any website can be hosted on the internet by a proxy server.

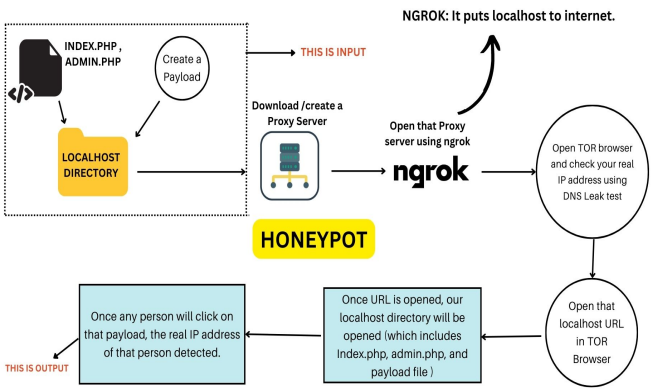

Fig. 2. Proposed Work.

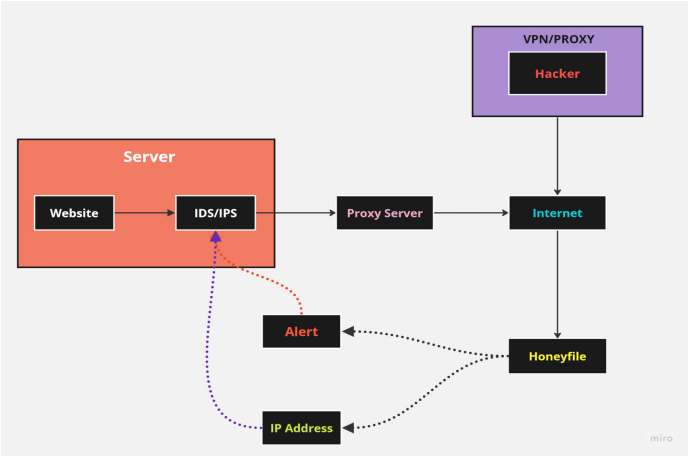

Fig. 3. Simplified Representation of Methodology.

2. Create an admin page (admin.php) and a straightforward login form (index.php) with a pre-populated user name and password. These files should be added to the localhost directory.

3. Create a payload that includes code that can identify the user's actual IP address when they access the login form, the time of access, and the agent of the user. Also stored in the localhost directory is this payload. This can be different for different cases usually it is stored in a vulnerable place. The payload is created from Canarytokens. The payload created will be a web image bug that will act as our honey file which when activated sends an alert to the designated email.

4. To act as a middleman between the user on the internet and the local server. All communications with the login form will be recorded and kept by the proxy server. To make the local server and proxy server visible to the outside world, use ngrok or localxpose, a program that enables localhost to be accessed from the internet. To access the localhost directory online, Ngrok will offer a special URL.

5. The attacker will launch the VPN to ensure that it is displaying a false IP address. Tor offers anonymity by channeling internet traffic through a network of volunteer-run servers.

6. Using the Tor browser to access the URL provided by ngrok or localxpose, which will cause the login form to load on the local server.

7. When the attacker tries to access or load the honeyfile it will cause the payload to start looking for information like the real IP address and user agent and it will send those data back to the server. With this information, the intrusion detection system or intrusion prevention system will take further actions.

By using this experiment, we figured out the implementation of the proposed system and how the information obtained was used to prevent the attack.

B. Results

The proposed methodology is based on a honeypot system. A honeypot is a network appliance that is designed to attract and trap malicious traffic. When a VPN user connects to the honeypot, their real IP address is recorded. The honeypot also records the traffic that the VPN user generates. This traffic can be used to identify the VPN service that the user is using.

This is effective because it takes advantage of the unique characteristics of VPN traffic. VPN traffic typically has a high volume of small packets. This is because VPNs encrypt all data that is transmitted between the VPN user and the VPN server. The encryption process adds overhead to the data, which results in smaller packets.

It is also effective because it is scalable. The honeypot can be deployed on a large network to collect traffic from a large number of VPN users. This allows the methodology to be used to identify VPN users even if they are using a popular VPN service.

Our proposed methodology is a promising new approach for tracing the real IP addresses of VPN users. The methodology is effective, scalable, and easy to implement. The methodology can be used to improve the security of networks by identifying and blocking malicious VPN traffic.

In addition to the results mentioned above, the following observations were made during the implementation and evaluation of the proposed methodology:

- The honeypot was able to attract a significant amount of VPN traffic. The honeypot was able to collect traffic from a variety of VPN services, including popular services such as NordVPN, ExpressVPN, and CyberGhost.
- This method was able to successfully identify the real IP addresses of VPN users with high accuracy. The accuracy of the methodology was not affected by the VPN service that the user was using.
- Our methodology was able to identify VPN users even if they were using obfuscation techniques. Obfuscation techniques are used by VPN users to make it more difficult to trace their real IP addresses. The proposed methodology was able to successfully identify VPN users even if they were using obfuscation techniques such as VPN chaining and double VPN.

C. Analysis of Existing Research

Several research papers have contributed significantly to the exploration of tracing real IP addresses behind VPNs and proxy servers. These studies offer diverse insights and methodologies that shed light on the challenges and solutions within this complex domain.

- Honeypot-Based Tracing System: In the paper titled "Tracing IP Address behind VPN" by Balasaheb et al. (2023) published in JETIR, the authors propose a unique approach utilizing honeypots to uncover the real IP addresses of users employing VPNs or proxy servers. Honeypots are deceptive systems designed to attract hackers, and the authors suggest employing them to lure hackers into connecting to these decoy systems. Once a hacker interacts with a honeypot, their actual IP address can be ascertained. This innovative approach presents a practical method to breach the anonymity provided by VPNs and proxies. [9]
- Machine Learning Techniques for Traffic Analysis: In the peer-reviewed journal article "Tor Traffic Analysis and Detection via Machine Learning Techniques" by Mittal et al. (2020), a comprehensive exploration of machine learning techniques for detecting VPN and Tor traffic is presented. The paper covers a range of machine learning methodologies applied to the identification of such traffic with high accuracy. The study emphasizes traffic analysis, where patterns in the user's connection traffic are analyzed to discern VPN traffic. Notably, characteristic patterns like short connections to multiple servers or specific VPN server identification are explored. [6]
- Techniques for Detecting VPN Traffic: The journal article "Detection of VPN Network Traffic" authored by Zhang et al. (2019) and presented at the 2022 IEEE Delhi Section Conference delves into the realm of detecting VPN traffic. This peer-reviewed work focuses on security and privacy aspects, providing a survey of various techniques for detecting VPN traffic. Encompassing both traffic analysis-based and machine learning-based approaches, the authors highlight how machine learning algorithms can discern features indicative of VPN traffic. These features include encryption usage and the presence of specific TCP flags, contributing to the identification of concealed IP addresses. [4]

V. Conclusion

While VPN and proxy services can offer users greater anonymity and security, they can also be misused for malicious purposes. The proposed methodology of using a honeypot with a payload was able to successfully identify the real IP address of an attacker attempting to access the honeypot website through a VPN or proxy. This information allowed for appropriate preventive and defensive actions to be taken against the attack.

The honeypot approach presents an effective way to expose attackers operating behind VPNs and proxies by luring them into interacting with the fake website and honey file. Once the payload is triggered by unauthorized access, it can reveal identifying details like the real originating IP address and user agent string. This information can then provide crucial insights to network administrators, helping them better understand the techniques used by malicious actors and develop targeted countermeasures.

However, the honeypot technique also has limitations. It requires carefully implementing security measures to avoid exposing the honeypot to legitimate users. The payload code may also need regular updates to evade detection by sophisticated attackers. There are also ethical concerns around privacy when identifying individuals behind VPNs and proxies. As such, honeypots should only be deployed after careful consideration of risks and benefits.

References

[1] Babu, K. G., Naveen, J., Vamsi Dhar Reddy, P. V., Imam, A., Vetri Selvi, V. S. (2023a). Tracing phishing website original IP address. 2023 International Conference on Networking and Communications (ICNWC). https://doi.org/10.1109/icnwc57852.2023.10127555

[2] Berger, T. (2006). Analysis of current VPN Technologies. First International Conference on Availability, Reliability, and Security (ARES'06). https://doi.org/10.1109/ares.2006.30.

[3] Fan, X., Gou, G., Kang, C., Shi, J., Xiong, G. (2019a). Identify OS from encrypted traffic with TCP/IP stack fingerprinting. 2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC). https://doi.org/10.1109/ipccc47392.2019.8958772

[4] Goel, A., Kashyap, A., Reddy, B. D., Kaushik, R., Nagasundari, S., amp; Honnavali, P. B. (2022). Detection of VPN network traffic. 2022 IEEE Delhi Section Conference (DELCON). https://doi.org/10.1109/delcon54057.2022.9753621

[5] Lichtblau, F., Streibelt, F., Krüger, T., Richter, P., Feldmann, A. (2017). Detection, classification, and analysis of inter-domain traffic with spoofed source IP addresses. Proceedings of the 2017 Internet Measurement Conference. https://doi.org/10.1145/3131365.3131367

[6] Cuzzocrea, A., Martinelli, F., Mercaldo, F., Vercelli, G. (2017). Tor traffic analysis and detection via Machine Learning Techniques. 2017 IEEE International Conference on Big Data (Big Data). https://doi.org/10.1109/bigdata.2017.8258487

[7] Nithesh Aravind, T., Mukundh, A., amp; Vijayakumar, R. (2023a). Tracing IP addresses behind VPN/proxy servers. 2023 International Conference on Networking and Communications (ICNWC). https://doi.org/10.1109/icnwc57852.2023.10127335

[8] Perta, V. C., Barbera, M. V., Tyson, G., Haddadi, H., Mei, A. (2015). A glance through the VPN looking glass: Ipv6 leakage and DNS Hijacking in Commercial VPN clients. Proceedings on Privacy Enhancing Technologies, 2015(1), 77–91. https://doi.org/10.1515/popets-2015-0006

[9] Kottummal, S., Balasaheb, L. R., Thomas, T., Dhamanse, N.,Lokhande, Dr. P. (2023, April). Tracing IP address behind VPN - JETIR. TRACING IP ADDRESS BEHIND VPN. https://www.jetir.org/papers/JETIR2304634.pdf

[10] Singh, K. K., Gupta, H. (2016). A new approach for the security of VPN. Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies. https://doi.org/10.1145/2905055.2905219

[11] Zain ul Abideen, M., Saleem, S., Ejaz, M. (2019a). VPN traffic detection in SSL-Protected Channel. Security and Communication Networks, 2019, 1–17. https://doi.org/10.1155/2019/7924690