VPN Detection and Blocking

Tejas Ravi Ghatikar and Vemuri Anvesh Sai

[1,2]UG Scholar Dept. of Information Science B.M.S. College of Engineering (affiliated to VTU) Bengaluru, India

.

Abstract—A huge opportunity for Blocking through Vpn address detection is to design a system specifically to support small-scale Websites in the process of achieving high level security from fraudulent activities. The ability to build an automated system to detect a Vpn-address and deny access in a cost effective manner helps reduce their vulnerability of being targeted. The prime goal of the proposed application is to solve the problem of website owners to safeguard their business from unethical activities such as piracy. Upon entering the website, the system will grant/deny access to user based on their IP address being a Vpn enabled IP-address or not. Hence, users who are trying to use Vpn to enter website will be denied access and shown a forbidden access page giving a choice to refresh and enter the website without a Vpn-enabled Ip address.

Keywords— Vpn- Ip address detection, Vpn blocking, Vpn detection, automate, Piracy

INTRODUCTION

First, a little information on how the world of the internet works: browsers, websites, service providers, and other devices may discover your public IP address. It opens the way for your confidentiality to be breached. It may also mean that information that is sensitive falls into malicious hands. When using a VPN, it uses the address of the VPN server from which all your internet traffic is routed instead of your public IP address being shown. This VPN server could be located anywhere in the world, making it difficult for those interested to find out your true location, let alone any personal details. The Virtual private network(VPN) market is projected to grow at a figure of 6.39% to reach US $50.153 billion by 2024, from US$34.591 billion.In the recent past, there have been a few significant instances of criminal activities by the use of Vpn, through mixing VPN and Windows bugs, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Protection Agency (CISA) said in a joint security warning that was issued in 2017. Hackers have obtained access to government networks. The observed attacks merged two Security vulnerabilities known as CVE-2018-13379 and CVE-2020-1472 according to the joint warning. The vulnerability enables attackers to take over domain controllers, server users to manage entire internal/enterprise networks, and typically requires passwords for all related workstations.

Indians are not new to circumventing bans by using the VPN path. The Department of Telecom (DoT) had previously requested internet service providers in October 2017 to ban 827 websites for allegedly hosting obscenity-realised content, which also prompted the use of VPN apps and website extensions. 91 percent of its visitors from India used VPN to access the website, according to the 2019 PH survey. This was despite two of India's largest telecom and internet service providers, Reliance Jio, Bharti Airtel and Vodafone Concept, having taken down the most obscene websites in many telecom circles on their network. The numerous data breaches that have been happening for the last number of years, such as the 2012 LinkedIn hack that was only discovered in 2016, are other attacks of note. Around 167 million account data were compromised, including emails and passwords. If the perpetrators who carried out these attacks used VPNs to conceal their identity, it could be difficult, if not impossible, to track them down. Knowing whether or not a VPN has been used may help to monitor those responsible for attacks such as those mentioned above The framework introduced in this paper aims to avoid fraudulent activities from taking place by automating the process of detection.

Upon accessing the website via a vpn enabled Ip address, the user will be denied access from our website as it is able to refuse access to the user based on the IPQUALITYSCORE API score that determines whether or not an ip address is based on Vpn. The intent of this website is to determine whether or not an incoming link to a web server originates from a VPN server

I. LITERATURE SURVEY

There have been several research works regarding the prevention of fraudulent activities on websites while some of them have shown various alternatives and relevant studies to Vpn Ip address detection.

Authors of [5] built a model that showed the efficacy of using a Multi-layered perceptron neural network model trained to identify incoming network traffic to a web server as either originating from an OpenVPN link or not, using TCP flow-based features. They have used technologies such as Wireshark for packet capture and Weka a tool used for classifying if the incoming traffic is from a VPN or not.

Further, In today's study, the authors of [6] have put forward yet another viewpoint where they have shown the use of blocking users of a website based on Internet legislation on online access by 10 countries with sensitive domestic problems and have imposed tight control over religious websites to avoid the dissemination of immoral propaganda. They created an application named WBF that conducts a search for a domain name server to check whether it matches the URL in the blocked list and offers a snapshot view of the blocking website in the restriction categories selected.

However, The authors of [7] have researched the efficiency of time-related features to tackle the difficult problem of encrypted traffic characterization and VPN traffic detection. Two C4.5 and KNN machine learning algorithms were used, achieving accuracy levels above 80%.

The authors of [8] talk about how blacklists of IP addresses rely on Web filters. Speed, basically a simple table lookup, is the key benefit of blacklists. Speed enables Web filtering at network choke points where traffic, such as gateways between neighbouring national networks, is aggregated. For proxy-based filters, IP and URL blacklists can be deployed. In all web requests, a proxy-based filter tests the IP addresses or URLs against a blacklist. If a blacklisted IP address or URL is detected, the proxy filter can return an error message to the block page or clarify that the content has been blocked.

However Authors of [9] suggested an alternative to website blocking by combining content-based filtering with URL filtering, using the Multiple Classification Ripple-Down Rules (MCRDR) method of acquisition of information, which enables the domain expert to maintain the knowledge base without the assistance of knowledge engineers. The MCRDR-based information filtering system can easily prevent the transmission of unknown web information and easily maintain the filtering system's knowledge base.

Authors of[10] demonstrated proxy detection methodology to incorporate such technology in a business solution with the sole purpose of removing the majority of fraudulent transaction attempts, evaluating various detection techniques with tools such as TORguard, Wireshark and RBL dataset data collection, gaining knowledge to design a multi-tiered proxy detection module which could give a detection rate of 97% .

The authors of[11] have built an active assessment framework to test the different infrastructure and privacy aspects of VPN services and to evaluate 62 business providers. The findings indicate that while commercial VPN services tend to be less likely to intercept or tamper with user traffic overall than other previously studied types of traffic proxying, many VPNs leak user traffic through a variety of means, perhaps inadvertently. They also found that a non-trivial fraction of VPN providers proxy traffic transparently, and many misinterpret the physical position of their viewpoints: 5-30 percent of the viewpoints, correlated with 10 percent of the viewpoints.

An automatic VPN bypass method for network virtualization was suggested by the authors of[12], enabling offshore business activities that need to bypass connectivity blocks in order to remain connected to motherland computers. The theory was based on the notion that the blocking process cannot be modified at will and that it is possible to recognize an RTT signature of the block onset. Via analysing the phenomenon, they find that the RTT Round Trip Time of Internet Control Message Protocol (ICMP) echo increases gradually from 1 h (recently mostly from 10 min) to several hours during GS blocks at the pitch of 50-500 ms per move .

II. RESEARCH METHODOLOGY

In order to detect the incoming connections and determine if they are Vpn enabled or not we aim to build a detection system which is cost effective and accurate. There are many advantages of using the approach of detecting an IP address for prevention of unethical activities but it comes with disadvantages, Currently some use URL filtering but URL filtering deployments, however, do not have the right mechanisms to properly control web browsing and prevent threats. They cannot coordinate actions and lack visibility of application and meaningful integration with other solutions required to protect against different attack phases and threat vectors.. For example, phishing sites may be detected via an IPS or even a sandbox, but with stand-alone URL filtering, lack of communication between sandbox, IPS and URL filtering technologies may result in insufficient protection of the URL request. Whilst there is a huge amount of valuable data to be gained from IP address tracking, there can sometime be problems with this data's accuracy and collection. Some IP address trackers that provide an IP address to users may draw data from public databases held by the ISP (Internet Service Provider) that originally assigned an IP address. This means that the data is often out of date, and it is less accurate to assume that the location This may still be of use to many marketers, especially when discovering geographic markets, you were unaware that you had penetrated. In order to overcome these limitations, the aim of this paper is to provide a better solution.

The primary objective of the proposed system is to create an environment that detects whether a user is trying to access the website via a Vpn-enabled IP address and to deny access to it by using efficient tools to obtain the most accurate results.

III. VPN DETECTION SYSTEM

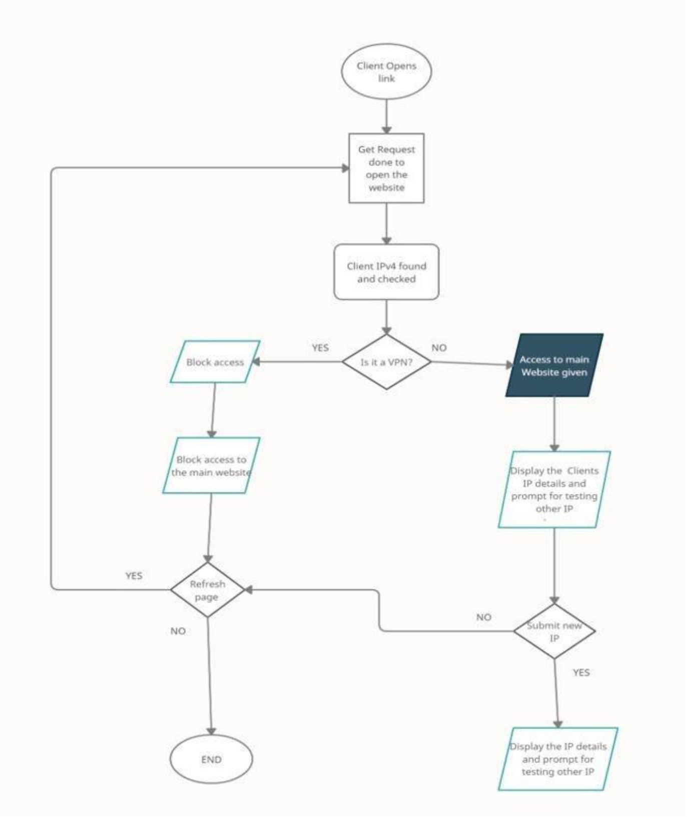
Client Opens link
Get Request done to open the website
Client IPv4 found and checked
Is it a VPN?
YES
NO
Block access
Access to main Website given
Block access to the main website
Display the Clients IP details and prompt for testing other IP
YES
Refresh page
NO
NO
Submit new IP
YES
END
Display the IP details and prompt for testing other IP

Fig .1. Complete block diagram of the proposed system Figure 1 explicates the state diagram of the system design being proposed. The explanation for each state is as follows:

A. IPQUALITYSCORE API

The IPQUALITYSCORE API uses machine learning models to predict the information points of a specific IP address and, as a result, displays the details of the IP address. The web application makes an API call when the user attempts to access the website based on the API SCORE, The IP address is identified as or not a proxy IP address and denied access to the website if the user's IP address is from a VPN and the prohibited access page is shown with the option of reconnecting a VPN. If the user accesses the website without using a VPN, the web application allows the user to query an IP address for details such as country code, region, city status and VPN status In this way, we successfully prevent the user from entering the website through a VPN and potentially prevent fraudulent activity from taking place.

B. Web Application

The web application acts as an user interface for the VPN detector system, the moment user tries to enter a website, it shown details regarding the users IP address such as country code, region and Vpn status. The web application has an additional feature where it prompts a form to query any IP address of your choice and displays details regarding the queried IP address.

C. Database

The system consists of a database to which answer scripts will be saved. Upon completion of the examination, the answer scripts can be retrieved by the school from the server. The server will store information related to the school - teachers' names and subject information, answer scripts, student information. MySQL is used to maintain the database. PHP is used to connect the web page and database.

IV. EXPERIMENT RESULTS AND EVALUATION

SI no	IP	VPN	Country Code	Region	City
1	5.5.5.5	False	DE	Bradenburg	Oegeln
2	43.247.159.8	False	IN	Karnataka	Bengaluru
3	181.233.103.0	True	CR	Heredia	Heredia
4	181.224.76.0	True	PA	Vereguas	Santiago de Vereguas
5	106.217.124.57	False	IN	Karnataka	Madikeri

1) Connection one is not using a VPN , the IP address detected shows VPN enabling to be False. The connection is identified and shows details of the city ,region and country code.
2) Connection two is not using a VPN , the IP address detected shows VPN enabling to be False. The connection is identified and shows details of the city ,region and country code.
3) Connection three is using a VPN,The IP address detected shows VPN enabling to be True which shows that the user is trying to access the website through proxy IP address and fake location.
4) Connection four is using a VPN,The IP address detected shows VPN enabling to be True which shows that the user is trying to access the website through proxy IP address and fake location.
5) Connection five is not using a VPN , the IP address detected shows VPN enabling to be False. The connection is identified and shows details of the city ,region and country code

V. RESULT EVALUATION

The API performed its function with efficiency and effectiveness. Various insights were obtained from the results. There was a total of 203 API calls made to retrieve the IP addresses details, out of which the average fraud score was found to be 7.0567 considering there were only there were only 10 IP addresses searched which was found to be VPN enabled IP address.

The majority of VPN detected IP addresses had their location spoofed to Canada,USA,China,Germany and United Kingdom.

VI. CONCLUSION

In today's world of increasing numbers of cybercrime cases, such as data breaches, cross-border streaming, phishing has seen the majority of fraudsters using VPN as a means of bypassing security systems and concealing their identity. This arises from the need for effective security measures to be implemented in a convenient manner. The threat of fraudulent activity on websites is a major concern for companies and the increasing cost of cyber security systems has made it difficult to decide which approach to take .Our system aims to prevent fraudulent activities from taking place by denying users access to the VPN website by detecting the user's VPN-enabled IP address. The results obtained show one of the highest accuracy when detecting VPN IP addresses that have been spoofed to countries such as Canada, the USA, China, Germany and the United Kingdom. The proposed system is also easy to integrate and user-friendly.

REFERENCES

[1] DATACONOMY-“Three vpn use cases you should know about” februrary 19 2020

[2] INC42 –“Indians expected to take vpn route to dodge Chinese app ban “ June 30 2020

[3] ZDNET-“hacker group chain vpn and windows bugs to attack us government networks” October 12 2020

[4] T. Hunt, “Observations and thoughts on the LinkedIn data breach,” troyhunt.com,2016.[Online].Available:”https://www.troyhunt.com/observations-and-thoughtson-the-linkedin-data-breach/”.[Accessed: 06-Dec2017].

[5] S. Miller, K. Curran and T. Lunney, "Multilayer Perceptron Neural Network for Detection of Encrypted VPN Network Traffic," 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), Glasgow, UK, 2018, pp. 1-8, doi: 10.1109/CyberSA.2018.8551395.

[6] Draper-Gil, G.; Lashkari, A.; Mamun, M. and A. Ghorbani, A. (2016).” Characterization of Encrypted and VPN Traffic using Time-related Features”.In Proceedings of the 2nd International Conference on Information Systems Security and Privacy - Volume 1: ICISSP, ISBN 978-989-758-167-0, pages 407-414. DOI: 10.5220/0005740704070414

[7] T. M. Chen and V. Wang, "Web Filtering and Censoring," in Computer, vol. 43, no. 3, pp. 94-97, March 2010, doi: 10.1109/MC.2010.84.

[8] Chen, Thomas & Wang, Victoria. (2010). "Web Filtering and Censoring". Computer. 43. 94 - 97. 10.1109/MC.2010.84.

[9] Churcharoenkrung, N.; Kim, Y.S.; Kang, B.H. (2005). [IEEE International Conference on Information Technology: Coding and Computing (ITCC'05) - Volume II - Las Vegas, NV, USA (2005.04.4-2005.04.6)] International Conference on Information Technology: Coding and Computing (ITCC'05) - Volume II - Dynamic Web content filtering based on user's knowledge. , (), 184–188 Vol. 1. doi:10.1109/itcc.2005.137

[10] M. Pannu, B. Gill, R. Bird, K. Yang and B. Farrel, "Exploring proxy detection methodology," 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF), Vancouver, BC, Canada, 2016, pp. 1-6, doi: 10.1109/ICCCF.2016.7740438.

[11] Mohammad Taha Khan, Joe DeBlasio, Geoffrey M. Voelker, Alex C. Snoeren, Chris Kanich, and Narseo Vallina-Rodriguez. 2018. An Empirical Analysis of the Commercial VPN Ecosystem. In <i>Proceedings of the Internet Measurement Conference 2018</i> (<i>IMC '18</i>). Association for Computing Machinery, New York, NY, USA, 443–456. DOI:https://doi.org/10.1145/3278532.3278570

[12] Fujikawa, H., Damiani, E., Yamamoto, Y. et al. Network virtualization by differentially switched VPN for stable business communication with offshore computers. J Reliable Intell Environ 2, 119–130 (2016). https://doi.org/10.1007/s40860-016-0026-