IS VPN GOOD TO USE IN TODAY's WORLD

Akshay Agrawal
Student, NCRD's Sterling Institute of Management Studies, Nerul, Navi Mumbai
akshayagrawal.mca@gmail.com

Priyanka B. Patil
Student, NCRD's Sterling Institute of Management Studies, Nerul, Navi Mumbai
priyankabpatil.mca@gmail.com

Prof. Sagar Thakare
Assistant Professor (MCA), NCRD's Sterling Institute of Management Studies, Nerul
sagthakare@gmail.com

ABSTRACT

In the modern world, we are constantly transmitting personal information over the internet without caring about any privacy whether we're logging into our bank account or just having a private conversation with our best friend, we don't want someone to snoops on us, that's where VPNs comes into the picture. VPN is a growing technology that allows us to create a secure way. People have begun working on remote devices that demand good protection and privacy. So, these days VPN will be the prime necessity for any individual organization and company. In addition, those concerned with their personal details, using VPN's will be their primary concern. They guarantee a degree of privacy for computers and Internet users in any part of the world. This paper's main aim would be to cover the major aspects of how to prevent user to access banned websites and restrict them to do illegal work without permission of local authorities and maintain privacy and security while using VPN.

Keyword: *VPN, Privacy, technology, Internet, restrict, Banned and Security*

2. INTRODUCTION

VPN is an acronym for Virtual Private Network. The purpose of a VPN is to give us with security and privacy as we transmit data over the internet from our office or from any remote location. Our Internet protocol address is shielded by VPNs so that our online activities are practically untraceable which makes it easier. So, these days VPN will be the prime necessity for every organization and company. The two most common reasons for using a VPN for personal use are to enhance the privacy and protection of the user, and to circumvent geographic restrictions or censorship. For business use, VPNs are widely used to give workers access to private company servers. VPN are the most favorable part of any IT industry because it establishes high secure communication from corporate-office to remote sites and remote users. VPN is growing very fast in the modern world due to the improvement in the modern technologies. People start to work remotely either from their home or some other places allocated to them. So, these days VPN plays a major role.

3. LITERATURE REVIEW

According to Saugat Bhattarai who is student of NAAMI- Computer Vision Research and Sushil Nepal from Kathmandu University, have researched on "Virtual Private Network" in the sense that it carries controlled information, protected by various security mechanisms, between known parties.**[2]**

A virtual private network is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.**[2]**

According to 'Jay H Simmons' is a senior editor and writer for VPNCrew shown some disadvantages: -

1. Using VPN Might Actually Be Illegal in Your Country.
2. You Might Have Performance Issues While Using the Private Network.
3. The VPN Service Might Monitor Your Activity and Use Your Data.
4. It Might Be Difficult to Set Up for Business Users.
5. It Might Add More Cost to Your Network Connection.**[4]**

'Rob Mardisalu' has explained 'VPN' deeply from basic to advance, how do it work and how to use it in different devices. **[1]**

'Steven J. Vaughan-Nichols' explained how to use VPN to protect internet privacy. such as IP security, Layer 2 Tunnelling Protocol, and Secure Sockets Layer and Transport Layer Security.**[3]**

4. PROBLEM DEFINITION

Nowadays, Users are taking advantage of VPN service to access banned website & do illegal activities which is restricted by the local government authorities and also privacy is becoming a major concern for users as well as business organizations around the globe. So, it makes sense that making of them are turning to use VPNs to protect their data and privacy. There are a lot of free VPNs available in the market. But as the VPN's are expensive and complicated software it requires a great deal of investment. They also need to be updated according to the new privacy policies and protocols. Free VPN providers need to cover their costs and have to get some profit from their users, so there can be a possibility that our data

won't be that secure as we think. The main issue while using a free VPN is that we are not aware whether our data is distributed to third parties for making a profit.

The first step in considering a right VPN is understanding the cost associated with it. If we value our privacy then it is recommended that we use a paid service. We should look for no log VPN. In a No log VPN, the network does not maintain any log of our activities including our personal details, our IP address or our search and download history. We should check the company's terms of service to check whether they keep a log of our online activities.

5. OBJECTIVE

Objective of this paper is to show how we can prevent users from accessing forbidden websites and not allowing them to perform illegal work while using a VPN. Think of all the time on the go, reading emails or checking the bank account If we are logged in to a private network requiring a password, any data transmitted during our online session could be vulnerable to aliens using the same network. VPN hides our browsing history, our IP address and location, where we stream, the device we use, our web activity and more. VPN enables access to various digital platforms, more freedom while using internet. Another instance where we can use vpn is to access the websites which are not accessible in different locations. With a VPN service, we can have the web traffic tunnelled to another location or a country and access those blocked websites in our area. VPN enables users to connect our laptop, tablet, personal computers to another device or another computer that allows us to access the internet. China's Great Firewall is a great example of the countries not providing open internet to the citizens. So, if some-one wants to access internet or some information, they need a VPN service to browse hassle free.

6. RESEARCH METHODOLOGY

To begin, we must determine whether the individual requesting VPN connection is an authorised user, only approved and registered users will be able to connect to VPN clients; otherwise, they must register and identify themselves & then users will be able to connect to VPN clients, The VPN app encrypts our data until it is available to the Internet service provider or any other public Wi-Fi network the data then travels through a tunnel and from the VPN server to our destination whatever it may be, for instance can be a normal google page or any sharing platform. The destination sees the data coming from the VPN server and its location and does not know the exact device which we are using or our current location

which indeed makes it safe and secure to use. VPN connection then will encrypt our data, our traffic which makes it difficult for anyone to trace the original server thus improving the anonymity and safety. The VPN application which we are using in our smartphone, tablet or our personal computer will run in the background, and we can access the internet normally without noticing any difference.

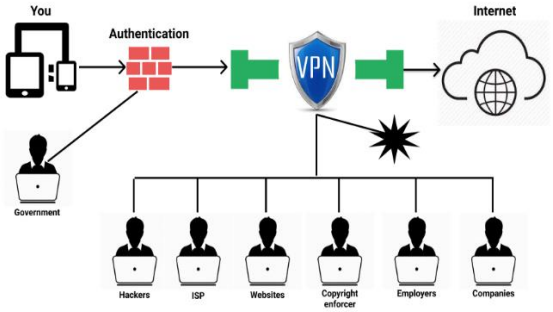

Fig. 1.1 Diagram

IV. TYPES OF VPN

There are two types of VPNs

- Wireless VPN
- Site-To-Site VPN

Wireless VPN:

Wireless VPN enables a user to safely and privately connect to a private network and access all of its services. It connects the user to a remote server which is secure. This type of VPN is secure for both home users and business users. The biggest benefit of this form of VPN is that they are very easy to set up and are free from hassle. This form of VPN is best suited to personal use.

Site-To-Site VPN:

The primary purpose of this form of VPN is to provide the ability to access the resources and data of each other to multiple users at various remote locations. Intranet based VPN are those VPN's where different offices of the same company are linked via Site-To-Site VPN. Extranet based VPN is used when businesses connect to another company's office.

TYPES OF VPN PROTOCOLS

Internet Protocol Security:

IPsec helps to protect network-wide internet contact. It uses communication via internet protocol by authenticating the session and encrypting each packet during the link. The difference between transport mode and tunnelling mode is that the transportation mode encrypts the data packet message while tunnelling mode encrypts the entire data packet.

Layer 2 Protocol on Tunnelling:

This protocol combines with other protocol to provide a stable link to the VPN. Layer 2 builds a tunnel between two connecting points and encrypts the data and manages secure tunnel communication.

Multi-protocol and Single Protocol VPN:

The main advantage of using multi-protocol VPN is that they provide a number of options to choose from. They offer various SSL/TLS encryption. Single Protocol VPNs are open source and currently considered the most secure option.

OpenVPN:

OpenVPN offers a custom encryption protocol based on the standard SSL and TLS protocol. It is used to build point to point connections, and Site to Server connections.

7. ANALYSIS FINDINGS

We have analysed that in today's world using of VPN is growing drastically in business environment & helping them to transfer data securely, In the other hand people taking disadvantage of the VPN to do illegal work & browsing websites which is banned by Government.

By this Authentication process we can check the legitimate user who can access the website & Local authorities can trace users who are engaging in corrupt practices or accessing banned websites and impose harsh measures against them.

for example, researchers have checked websites which are banned by local authorities without using VPN, user is unable to access it and if user connect to vpn, then user can access that website and do whatever he/she wants to do without interruption and knowing to anyone. Some website which is banned by Indian Government but can be access connecting to VPN

- https://www.tiktok.com/
- http://xpau.se/

Using VPN Chrome Web extension '**ZenMate'** this extension is gives 7 days free trail with limit location. To access full product feature, need to buy paid version.

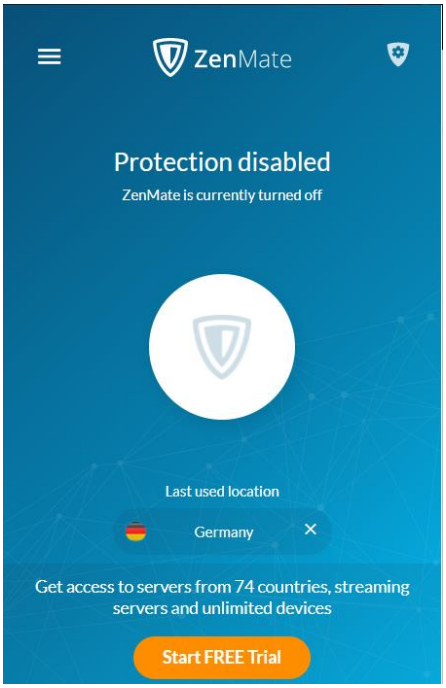

Fig. 1.2 Web VPN

8. LIMITATION

- Illegal use of VPNs themselves
- It Might Be Difficult to Set Up for Business Users
- A slower internet connection
- The VPN Service Might Monitor Your Activity and Use Your Data
- Connection breaks
- Using It Can Not Guarantee 100% Anonymity

9. CONCLUSION

The internet usage is going to rise with the increase in modern technologies. Usage of internet consumption has increased drastically and that leading to many privacy and security threats, we should understand the importance of VPN along with their pros and cons. Always use a paid VPN as they will be having more advanced features, customer support, network security, access to more geographic locations and better experience. As a user, we need to understand the policy of different locations and we should act accordingly.

10. REFERENCES

1. https://thebestvpn.com/what-is-vpn-beginners-guide/
2. https://www.researchgate.net/publication/289120789_VPN_research_Term_Paper
3. https://www.zdnet.com/article/how-to-use-a-vpn-to-protect-your-internet-privacy/
4. https://www.vpncrew.com/5-disadvantages-of-vpn-that-you-should-know-before-using-it/
5. https://vpnoverview.com/vpn-information/what-is-a-vpn/
6. https://searchnetworking.techtarget.com/definition/virtual-private-network