IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 6, June 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306195|

Is VPN an All-in-One Solution for Online Safety, Security, and Privacy?

Raghav Khadakkar, Omprakash Mandge

Student, Institute of Computer Science, Mumbai Educational Trust, Mumbai, Maharashtra, India

Professor, Institute of Computer Science, Mumbai Educational Trust, Mumbai, Maharashtra, India

ABSTRACT: Image In the digital age, security is very essential but people are relying upon Virtual Private Networks (VPN) to secure them online across the world. VPNs keep your information secret by protecting it against cyber threats; also ensuring that your privacy remains unknown; is there any possibility that by using VPNs all our safety needs will be met truly? Let's take a look at what the benefits and pitfalls of VPNs are, and see how the cybersecurity landscape keeps evolving. Are VPNs safe?

KEYWORDS: Virtual Private Networks (VPN), Tunnel, Internet, Encryption, Decryption, Remote Access, Site-to-Site, Server, Privacy, Online Safety, Security**.**

I. INTRODUCTION

The internet has revolutionized communication, commerce, and access to information. However, this revolution has come with significant risks, including data breaches, cyber-attacks, and privacy invasions. Virtual Private Networks (VPN) is a service that creates a private and secure connection to the internet. it establishes an encrypted tunnel between your computer and a remote server allowing some or all of your network traffic to be routed through that server before it goes to its destination. As users seek to protect themselves online, VPNs have gained prominence as a tool to enhance security and privacy. The purpose of VPN is to provide the different security elements such as authenticity, confidentiality, and data integrity that's why these are becoming trendy, low-priced, and easy to use. This paper analyses the role of VPNs in the broader context of online safety and evaluates their effectiveness as a comprehensive solution.

II. UNDERSTANDING VPNS

- HISTORY

Several years ago, the most common way to connect computers between multiple offices was by using a leased line. Leased lines, such as ISDN (integrated services digital network, 128 Kbps), are private network connections that a telecommunications company could lease to its customers. VPN access was a new concept to most businesses. Their origin can be found in Virtual Circuit. Virtual Circuit service is considered superior to a connectionless service for handling long messages. Virtual circuits are easy to implement in highly connected networks as well as being cost effective The virtual circuit was originally produced in the late seventies and early eighties. The basic structure of the virtual circuit is to create a logical path from the source port to the destination port. As businesses became more reliant on online operations, there was an urgent need to secure data. Initially, companies gravitated toward wide area networks (WAN) for security, but high costs led them to explore VPNs. Notably, during this period, James Yonan developed OpenVPN for personal use. This open-source protocol, along with the SSL VPN, became prominent solutions for businesses. During the mid-2000s, individual users became more aware of online security. Public networks, particularly in cafes and airports, turned into hunting grounds for hackers. Consequently, the need for online privacy tools surged among individual internet users, too. By 2005, recognizing the need for user-friendly security tools, the first commercial VPNs appeared, simplifying the previously complex setup processes. The decade concluded with VPNs evolving as essential tools, leading to an increase in third-party VPN service providers and innovative protocols like IKEv2/IPsec and SSTP.[1]

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306195|

- Definition, Functionality, and Offerings

A VPN is a technology that creates a secure and encrypted connection over a less secure network, typically the Internet. It is a networking framework that is effective over public networks to secure confidential data shared on the public network i.e., Fig A . It allows users to send and receive data as if their devices were directly connected to a private network, thereby enhancing security and privacy. VPN does two things it obscures your IP address helping hide your physical location from the sites and services that you use online and if it's properly configured it encrypts all your internet traffic including services like DNS concealing your browsing habits from your ISP and by extension any entity like a government or special interest group who might compel them to share that data. Most commercial VPN providers also offer extras like ad-blocking antivirus password managers remote access and even dark web monitoring but none of that is the VPN it's just add-ons to entice you away from the competition in a very competitive Marketplace. VPNs achieve this through several key components:

- Encryption: VPNs encrypt data transmitted over the internet, making it unreadable to unauthorized parties.
- Tunneling: Data is encapsulated in secure tunnels, preventing interception during transmission.
- Authentication: VPNs authenticate users and devices to ensure that only authorized entities can access the network.

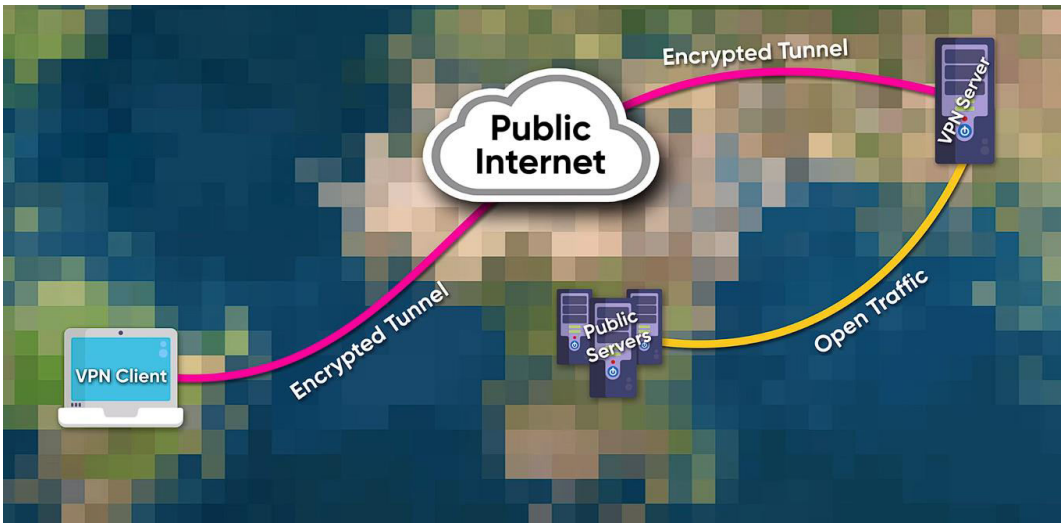

Fig A

III. TYPES OF VPNS

VPNs can be broadly categorized into:

- Remote Access VPNs:

A remote access virtual private network (VPN) enables users who are working remotely to securely access applications and data that reside in the corporate data center and headquarters, encrypting all traffic users send and receive i.e., Fig. B.

A secure remote access VPN creates a tunnel between the network and a remote user that is virtually private. Traffic is encrypted, which makes it unintelligible to eavesdroppers. Users in remote locations can securely access and use the network in much the same way as in the office. Using remote access VPNs, data can be transmitted without the risk of interception or tampering.[2]

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306195|

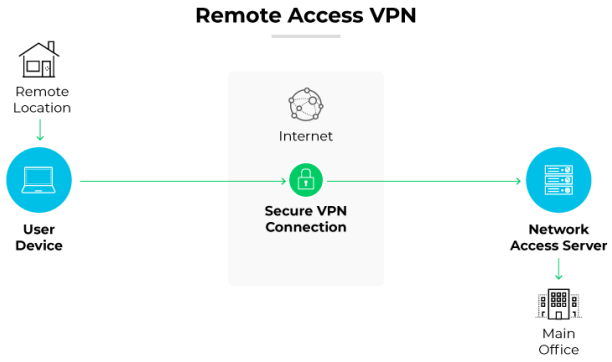

Fig. B

- Site-to-Site VPNs:

A site-to-site virtual private network (VPN) refers to a connection set up between multiple networks. This could be a corporate network where multiple offices work in conjunction with each other or a branch office network with a central office and multiple branch locations i.e., Fig. C.

Site-to-site VPNs are useful for companies that prioritize private, protected traffic and are particularly helpful for organizations with more than one office spread out over large geographical locations. These businesses often have to access resources housed on a primary network, which could include servers that facilitate email or store data.[3]

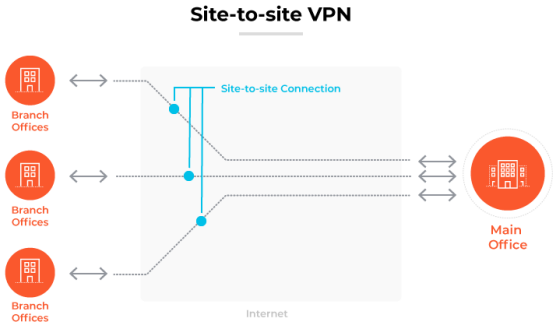

Fig C

IV. IMPORTANCE OF VPNS IN ONLINE SAFETY, SECURITY, AND PRIVACY

VPN can be an incredibly powerful and versatile tool which is why virtual private networking has been built into Windows for almost 30 years but number of other protections that you should have in place before ensuring total privacy and security.

Enhancing Security:-

VPNs provide several security benefits like

- Data Protection:

By encryption, tunnelling and authentication, VPNs protect sensitive information from being accessed by hackers.

- Secure Connections:

VPNs create secure tunnels for data transmission, reducing the risk of data interception.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306195|

- DNS leak protection:

All DNS requests through encrypted DNS servers. You can also configure your VPN to only connect to its own DNS servers, forcing your device to use the VPN's DNS instead of your ISP's. By routing your DNS queries through the encrypted tunnel and not relying on third-party DNS providers, they ensure that your browsing activity cannot be exposed by leaks from DNS queries.

- Full disk encryption:

Full disk encryption protects server certificates and all other configurations and software stored on our exit servers so that attackers cannot access any data, even if one was somehow compromised. This helps protect them against resource-intensive man-in-the-middle attacks that governments can perform.

- VPN kill switch:

In case a VPN connection drops, the user's internet access will switch to their regular connection. A VPN kill switch feature automatically exits specific programs if an internet connection becomes unstable to reduce the risk of sensitive data being leaked by applications.

- Multi-factor authentication (MFA):

Any VPN program should be as secure as possible to ensure that only authorized users can gain access to it. MFA enables a user to prove their identity, that they are who they say they are, before they are given access to the VPN.

Ensuring Privacy:-

VPNs enhance user privacy by

- Hiding IP Addresses: VPNs mask users' IP addresses, making it difficult for third parties to track online activities.
- Preventing Data Collection: VPNs prevent ISPs and other entities from collecting and monetizing users' browsing data.
- NO logs policy: It is a commitment by a VPN provider to not collect or store any data about a user's online activity. This means that the VPN provider cannot see what websites a user visits, what files they download, or what apps they use. This allows us to ensure that your private browsing history stays private and cannot be turned over to a third party under any circumstances.

Access to Restricted Content:-

VPNs can bypass geo-restrictions and censorship by allowing users to connect to servers in different locations. This feature is beneficial for accessing content unavailable in certain regions and for maintaining open internet access in countries with strict censorship laws.

V. OWNERSHIP AND TRUST CONCERNS

The ownership of VPN services is a critical factor in their reliability and trustworthiness. Recent analysis reveals that a significant portion of the VPN market is controlled by a small number of companies. For example, 105 VPN services are owned by just 24 companies[4], many of which operate in high-surveillance countries like China and Russia. This concentration raises concerns about data privacy and security, as companies in these jurisdictions may be compelled to share user data with their governments.

- Data Privacy Risks

If VPN providers are based in or owned by entities in countries with stringent data retention laws or surveillance practices, user data could be compromised. VPN services owned by companies in the Fourteen Eyes alliance countries are subject to potential government data requests, which could undermine user privacy. Additionally, companies operating in authoritarian regimes may be required to provide user data to the authorities, posing significant privacy risks [5].

- Fourteen Eyes alliance[5]

It is an alliance of 14 different countries that have agreed to share their intelligence. Its origin goes back to 1943 when an agreement was reached between the British and the US on a Communication Intelligence agreement. It originally started with only 5 countries and was known as the BRUSA agreement. After that, the program grew to 9 countries and now includes 14 total countries. In addition to these 14 countries, other supporting countries are not official members but regularly contribute to its network. The 14 Eyes alliance includes:

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306195|

1. Australia
2. Canada
3. New Zealand
4. United Kingdom
5. United States
6. Denmark
7. Netherlands
8. France
9. Norway
10. Germany
11. Belgium
12. Spain
13. Sweden
14. Italy

In addition to these members, other countries are considered partners or affiliates of the Fourteen Eyes Alliance. These additional countries include:

1. Israel
2. Japan
3. South Korea
4. Singapore
5. British Overseas territories (e.g. British Virgin Islands)

The reason the Fourteen Eyes Alliance is such a problem is that it allows governments to spy on their citizens by using other countries as a proxy.
For ultimate safety, a VPN shouldn't operate in any of the 5, 9, or 14 Eyes alliance countries. A privacy-friendly jurisdiction means there's no push to collect your data or what you do while the VPN is turned on. As such, locations like Panama, Switzerland, and Romania.

- Data Security Risks

The security of user data also depends on the practices of the VPN provider. Some providers have been found to engage in dubious practices such as logging and selling user data, embedding third-party trackers, or even compromising user devices with malware. Free VPN services are particularly notorious for such practices, highlighting the importance of selecting reputable and trustworthy providers.

VI. LIMITATIONS OF VPNS

An inconvenient truth of the VPN industry is, without additional layers of protection like torrent protocol encryption your VPN provider has a pretty good idea of where you go and what you're up to and all of that is only as secure as their willingness and ability to protect you which requires a lot of trust without much ability for the average person to verify. Despite their benefits, VPNs have limitations that prevent them from being an all-encompassing solution:

- Performance Impact: The encryption process and routing your traffic through remote servers can slow down your internet connection. However, premium VPN services usually have fast protocols and a powerful infrastructure that makes the speed drop barely noticeable.

- Trust Issues: Users must trust VPN providers with their data, and not all providers have transparent or trustworthy practices. The lack of transparency in logging policies and data handling practices can pose significant risks to user privacy. VPN security is the most important aspect of the service. Secure VPNs use strong encryption protocols and don't track or sell your browsing data. However, some free VPNs might be unsafe and do more harm than good. If a VPN service is free, it likely monetizes its operations by collecting your data and selling it to third parties or flooding you with ads. Free VPNs also tend to have a smaller server infrastructure, which results in

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306195|

congested servers and, consequently, slower speeds. Besides, they may have more security holes and weak encryption algorithms — the perfect recipe for data leaks.[6]

- Limited Protection: VPNs do not protect against all types of cyber threats, such as malware and phishing attacks. Relying solely on a VPN can give users a false sense of security, making them vulnerable to other types of cyber threats.

VII. COMPLEMENTARY TOOLS AND PRACTICES

To achieve comprehensive online safety, security, and privacy, VPNs should be used in conjunction with other tools and practices:

1. Usage of throwaway emails from a provider with strong privacy protections
2. Choose a VPN that has a long history of not just refusing to provide data logs to entities who demand them but being unable to (no data logging policy).
3. Usage of Tor
   Tor (The Onion Router) is a web browser that lets users access a network that anonymizes web traffic to provide private web browsing.
4. Usage of browser extensions for ad-blocking and
5. Decentralized VPNs

Decentralized VPNs (decentralized virtual private networks, or dVPNs) are VPN services that don't have a single entity for centralized control of their server network. Instead of having a VPN provider in charge of the network, volunteers operate individual nodes in the network. A decentralized VPN encrypts and routes your online traffic through multiple nodes.

VIII. BEST VPN SERVICES

Here are some of the top rated VPN service providers[7]

1. NordVPN
Company location: Panama
Number of servers: 6300
Number of countries covered: 111
Avg. download speed: 470 Mbit/s

2. Surfshark VPN
Company location: Netherlands
Number of servers: 3200
Number of countries covered:100
Avg. download speed: 443 Mbit/s

3. ExpressVPN
Company location: British Virgin Islands (BVI)
Number of servers: 3000
Number of countries covered: 105
Avg. download speed: 151 Mbit/s

4. Proton VPN
Company location: Switzerland
Number of servers: 5100
Number of countries covered: 91
Avg. download speed: 480 Mbit/s

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306195|

IX. CONCLUSION

What a VPN isn't though is some kind of all-in-one solution for Online safety security and privacy. Their effectiveness is maximized when used alongside other cybersecurity measures and practices. VPNs are a critical component of a multi-layered defence strategy, providing essential benefits but requiring complementary tools and practices to ensure comprehensive security. VPN doesn't give you some kind of digital diplomatic immunity and they don't make illegal activities any more legal they're just one piece of your broader digital privacy toolkit.

REFERENCES

1. Palo Alto Networks. "History of VPN." Palo Alto Networks, https://www.paloaltonetworks.com/cyberpedia/history-of-vpn. Accessed 22 June 2024.
2. Palo Alto Networks. "What Is a Remote Access VPN." Palo Alto Networks, https://www.paloaltonetworks.com/cyberpedia/what-is-a-remote-access-vpn. Accessed 22 June 2024.
3. Palo Alto Networks. "What Is a Site-to-Site VPN." Palo Alto Networks, https://www.paloaltonetworks.com/cyberpedia/what-is-a-site-to-site-vpn. Accessed 22 June 2024.
4. VPNpro. "Hidden VPN Owners Unveiled: 97 VPNs & 23 Companies." VPNpro, https://vpnpro.com/blog/hidden-vpn-owners-unveiled-97-vpns-23-companies/. Accessed 22 June 2024.
5. GOOSE VPN. "The 5 Eyes, 9 Eyes, and 14 Eyes Alliances: How Do They Lead to Our Privacy?" GOOSE VPN, https://goosevpn.com/blog/the-5-eyes-9-eyes-and-14-eyes-alliances-how-do-they-lead-to-our-privacy. Accessed 22 June 2024.
6. NordVPN. "Benefits of VPN." NordVPN, https://nordvpn.com/blog/benefits-of-vpn/. Accessed 22 June 2024.
7. VPNpro. "Best VPN Services." VPNpro, https://vpnpro.com/best-vpn-services/. Accessed 22 June 2024.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details