

Virtual Private Network: Survey and Research Challenges

Sudipti Banerjee., Dr. Rajni Ranjan Singh Makwana

Computer Science and Engineering Department Madhav Institute of Technology and Science Gwalior, India

DOI: <https://doi.org/10.51583/IJLTEMAS.2025.140600028>

Received: 17 June 2025; Accepted: 18 June 2025; Published: 07 July 2025

Abstract: The Virtual Private Network (VPN) is a rapidly developing technology that has a crucial function in guaranteeing the secure transfer of data. A virtual linkage is created among geographically distant individuals and networks that are linked through a common or public network, such as the Internet. Despite the fact that data is transmitted via a public network, a Virtual Private Network (VPN) signifies that the data is conveyed through a secure and private connection. Virtual Private Network (VPN) technology enables secure communication between two hosts by creating virtual tunnels. Upon the establishment of a tunnel, it becomes possible to transmit data between the two servers. This paper provides a comprehensive analysis of Virtual Private Networks (VPNs), including their historical background, architectural design, employed protocols, and identified vulnerabilities. A Virtual Private Network (VPN) is implemented to secure the private network by utilising encryption and other security measures, thereby ensuring that solely authorised users are granted access to the system and preventing data interception. This survey comprehensively covers the topics of Virtual Private Networks (VPNs), their protocols, and the security measures implemented within VPNs. The present article has conducted an overview of the diverse protocols employed in the domain of Virtual Private Networking.

Index Terms: VPN, Security Protocols, Tunneling, Remote Access, Tunnel Mode, and Transport Mode.

I. Introduction

Currently, network security has emerged as a crucial issue that requires attention. The Internet has significantly enhanced the accessibility of various facets of life, such as banking, shopping, communication, and the functioning of businesses and other entities [15]. The safeguarding of confidential information that is stored or transmitted via the internet is imperative owing to the nature of the communication network. The rapid proliferation of electronic devices and their integration with the Internet has led to an increased susceptibility of users' data to compromise. The complexities of data security and privacy risks are increasing, highlighting the necessity for a contemporary safeguarded platform that can ensure the protection of sensitive data transmitted through the Internet. The Internet is characterised as a network environment that is both public and lacking in protection. Companies and organisations leverage the vast potential of the Internet to construct computer systems that facilitate communication and data sharing within business platforms. The objective is to consistently establish an effective and protected operational milieu by safeguarding the assets of the establishment, a pursuit that is pursued on a daily basis. Businesses endeavour to identify pragmatic solutions to safeguard their network architecture against the infiltration of untrustworthy entities and cybercriminal activities during the design phase.

In contemporary times, the significance of data security cannot be overstated due to the prevalence of online business transactions and wireless communication, which are more susceptible to security breaches compared to computers linked to an internal network. Due to the possibility of interception by unauthorised parties, significant efforts are currently being devoted to data encryption and secure transmission. The primary objective of this study is to evaluate the existing security and encryption technologies of VPNs.

The task of analysing and identifying encrypted network traffic associated with specific applications and protocol configurations poses a significant challenge for network administrators. A multitude of network users utilise diverse encryption techniques on network applications and services in order to obfuscate the true intent of network communication. The collaborative efforts of the network community are promoted to enhance both network security and service quality.

A Virtual Private Network (VPN) is a communication network that utilises various technologies to facilitate secure data transfer over public or unsecured networks. The establishment of a virtual linkage among individuals and networks that are geographically dispersed can be achieved through the utilisation of a common or communal network, such as the Internet, for the purpose of interconnecting them. This would enable virtual connectivity between them. It appears that data is being transmitted through a secure channel as a result of the utilisation of a Virtual Private Network (VPN), which conceals the fact that it is being transferred over a public network. This document presents a survey study that encompasses VPN security and other related technologies within the same domain.

As expounded in this scholarly article, Virtual Private Network (VPN) technology is a commendable strategy for fortifying devices and data against malevolent hackers. It is strongly advised. A Virtual Private Network (VPN) is a secure communication channel that utilises a public network infrastructure to transmit encrypted data, thereby preventing unauthorised interception by malicious entities. The usage of Virtual Private Networks (VPNs) is on the rise. The increasing popularity of VPNs can be attributed to their ability to provide various security features, including authenticity, confidentiality, and data integrity, in a cost-effective and uncomplicated manner. Virtual Private Networks (VPNs) primarily address matters pertaining to the safeguarding of data privacy and confidentiality. A VPN, short for virtual private network, is a type of network that

expands on a private network by encapsulating data packets with headers on both ends of the communication line. This process involves using a combination of protocols on both ends of the communication channel to create communication tunnels. The nomenclature assigned to this category of network is a virtual private network (VPN). Virtual Private Networks (VPNs) can be considered as an additional security measure for confidential networks. Virtual Private Networks (VPNs) can be accessed through a range of devices, such as mobile devices, desktop computers, and tablets.

The development of innovative techniques for detecting intrusive network behaviour is a crucial area of investigation in the realm of network security, representing a notable research obstacle within the discipline. Numerous computational algorithms have been developed for the purpose of identifying unforeseen intrusions. However, the verification of dubious actions and the identification of their unique features continue to present significant challenges. Several data visualisation techniques have been devised to address this constraint, with the aim of enhancing the user's visual comprehension of data. Conversely, the extent to which visualisation techniques are efficacious in the analysis of network traffic data has not been extensively investigated.

Features of Vpn

1. One can establish network connections across multiple geographic regions without the requirement of a leased line.
2. By employing encryption techniques, it is feasible to enhance the mechanism of safeguarding data.
3. One of the advantages of this technology is that it enables remote offices and employees to connect to the company's intranet through an already established Internet connection, granting them equivalent flexibility to that of being physically connected to the network.
4. The possibility of time and monetary savings may be present for employees who work remotely.
5. Virtual Private Networks (VPNs) are becoming increasingly popular as a cost-effective alternative to leased lines, particularly due to the high expense associated with leased lines and the growing geographical separation between office locations.
6. IPSec VPN and SSL VPN are two commonly employed Virtual Private Network (VPN) solutions in wireless networks.

Our intention is to conduct a comprehensive examination of both, taking into account their advantages and disadvantages.

Utility of Vpn

7. Virtual Private Networks (VPNs) offer two notable advantages, namely cost-effectiveness and scalability.
8. Virtual Private Networks (VPNs) can reduce expenses by eliminating the necessity for expensive long-distance leased lines that would otherwise be mandatory.
9. To establish a secure private connection over the public network, it is sufficient to utilise a local leased line or a broadband connection to access the Internet and leverage its capabilities for tunnelling purposes.
10. Data transmissions are safeguarded through the utilisation of encryption.
11. The expenditure associated with the execution of this approach is negligible.

Limitations of Vpn

12. The Virtual Private Network (VPN) connection exhibits a suboptimal level of performance in terms of speed and responsiveness.
13. Due to the fact that the connection is established over public networks, it is imperative to possess a comprehensive understanding of network security issues and the necessary precautions prior to deploying a VPN.
14. The primary factor that influences the stability of a VPN connection is the scalability of the Internet, which is subject to external circumstances beyond the control of an enterprise.
15. The potential lack of interoperability among various VPN technologies may arise due to the underdeveloped nature of the standards.
16. The user is experiencing technical difficulties due to malfunctioning equipment and a sluggish internet connection.

History of Vpn

The development of Virtual Private Network (VPN) technology has been a gradual process over a significant period. The Virtual Circuit system can be considered as the precursor to its modern-day counterparts. Virtual circuits can be established with ease and at a low cost in networks that are closely interconnected. We will illustrate that Virtual Private Networks (VPNs) can also reap the advantages of these benefits. The virtual circuit was first created during the late 1970s and early 1980s. Currently, individuals continue to utilise it. The process of establishing a virtual circuit entails the formation of a logical linkage between the source port and the destination port, as depicted in the accompanying diagram. The establishment of the circuit may necessitate a considerable number of hops between routers along the path. The ultimate logical route or virtual circuit operates similarly to a

direct link between the two ports. Consequently, it is possible for two programmes to establish a connection by means of a shared network. The integration of encryption functionalities into router systems represented a significant achievement in the advancement of virtual-circuit technology. The advanced technology utilized encryption to secure the transmission of data between the virtual circuit's ports. Consequently, malevolent actors would be rendered incapable of gaining entry to information during its transmission between the communicating entities. Subsequently, supplementary security protocols, such as token authentication, were implemented. Regrettably, the channels of correspondence remained susceptible to unauthorised access, prompting the creation of a Virtual Private Network (VPN) that ensures secure communication across a publicly accessible network.

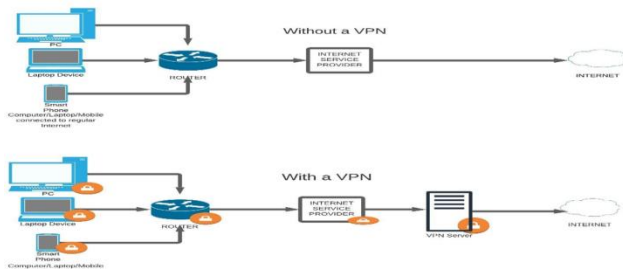


Fig. 1. Network Connection with and without VPN

Table I Most Commonly used VPN

PROVIDER	COUNTRIES	DEVICES	P2P
<i>Cyber Ghost</i>	61	7	Yes
<i>NordVPN</i>	59	6	Yes
<i>ExpressVPN</i>	94	5	Yes
<i>Surfshark</i>	50	Unlimited	Yes
<i>Hotspot Shield</i>	22	5	Yes
<i>HIDEMYASS!</i>	210	5	Yes
<i>purevpn</i>	141	5	Some
<i>privateinternetaccess</i>	25	5	Yes
<i>SAFERVPN</i>	34	3	No
<i>vyprvpn</i>	65	Upto 5	Yes
<i>Tunnel Bear</i>	20	5	No
<i>STRONG VPN</i>	21	1	Yes
<i>Stick VPN</i>	46	5	Yes
<i>IP VANISH</i>	60	5	Yes

Vpn Architecture

Prior to delving into the analysis of the architecture of virtual private networks (VPNs), it is imperative to acquire a comprehensive comprehension of the fundamental mechanisms that facilitate their operation. Instances of technological progressions encompass tunnels, firewalls, and proxy servers. The fundamental element of a conventional VPN architecture is constituted by tunnels, while supplementary components such as firewalls and proxy servers may be incorporated as discretionary features. This text provides a concise overview of firewalls and proxy servers, as well as an introductory discussion on tunnelling technology.

Tunnelling, which is also referred to as encapsulation, is a technique used to enclose a network packet within another. A transit packet refers to a packet that has been encapsulated within another packet, whereas a tunnelled packet denotes a packet that has been encapsulated within another packet. At the connection level, which is the lowest tier of the OSI model, all data contained within the packet is subject to encryption. The concept of encapsulation, similar to virtual private networks (VPNs), has been in existence for a considerable period. The technology has been employed to establish connectivity between disparate Internet domains that exhibit distinct functionalities or regulations compared to the broader network. The tunnel functions as a routing mechanism and provides an additional layer of security atop the Internet protocol. Encapsulation can be

achieved through a series of straightforward procedures. In order to establish a secure tunnel, it is necessary to append an additional IP header to the original one. The tunnel's security data is then inserted between these two headers. The initial packet's sender and recipient are specified by the inner header, while the tunnel's endpoints, also known as the source and destination, are indicated by the outer header.

Types Of Vpn

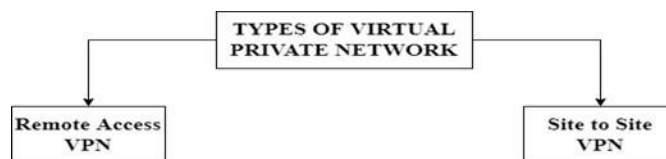


Fig. 2. Types of VPN

REMOTE ACCESS VPN - A system that enables remote access. The establishment of a VPN connection is the responsibility of a remote access client. A remote access client refers to an individual user operating a single computer who initiates a connection to a private network from a location that is geographically separate from the original point of connection. The Virtual Private Network (VPN) server facilitates user access to network resources connected to the VPN server through a secure and encrypted connection. The VPN client is responsible for initiating the packets that traverse the VPN connection. Prior to enabling mutual authentication, it is necessary for both the VPN client and VPN server to undergo authentication procedures. The process of establishing a secure connection between the VPN client and server requires mutual authentication, whereby both parties must verify their identities to each other.

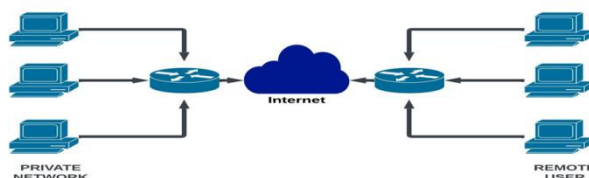


Fig. 3. Remote Access VPN

SITE – TO – SITE VPN - A virtual private network (VPN) connection established between two distinct segments of a private network or between two distinct private networks is referred to as a site-to-site VPN connection. By means of the internet, a corporation can establish routed connections with multiple offices and other enterprises. Theoretically, a Virtual Private Network (VPN) connection that is routed through the Internet can offer the same level of performance and reliability as a dedicated Wide Area Network (WAN) link.

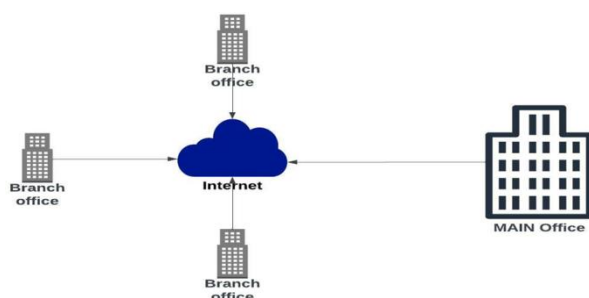


Fig. 4. Site-to-Site VPN

Operating Principle

It is conceivable that corporations may need to overcome the primary impediments in order to utilise the internet as a replacement for their proprietary wide area networks (WANs). Commencing with the topic at hand, despite the fact that networks often engage in communication with each other through diverse protocols, including IPX and NetBEUI, it is noteworthy that the Internet solely possesses the capability to handle messages that are founded on IP. The reason for this is that the Internet Protocol (IP) is the sole protocol that is capable of addressing the decentralised structure of the Internet. The implementation of virtual private networks (VPNs) may be necessary to facilitate the transfer of non-IP protocols between networks. In addition, data packets containing plain text are transmitted through the Internet. Consequently, individuals with access to the traffic of the Internet possess the ability to peruse the data encapsulated within the packets. Organisations intending to employ the Internet as a medium for transmitting confidential and critical business data must take cognizance of this issue. Tunnelling is the mechanism by which

virtual private networks (VPNs) circumvent these obstructions. The encryption of data packets is performed as a safety measure prior to their encapsulation in an IP package by the virtual private network (VPN) and subsequent transmission through the public Internet. This occurs prior to the transmission of the packets through the Virtual Private Network. Assuming the scenario of NetWare being operated on a single network, a client located on the same network expresses the desire to establish a connection with a NetWare server situated in a geographically distant location. What would be the potential outcome? What would be the potential outcome? Please consider the following hypothetical situation. The primary protocol utilised in conjunction with conventional NetWare is IPX. The transportation of IPX packets towards the distant network is facilitated through a tunnel initiation mechanism. This mechanism may take the form of a router, a remote access device, or a desktop PC, depending on whether the connection is between a remote client and server. The method employed is based on a generic layer-2 VPN model. This hardware device facilitates the organisation of data packets to ensure their readiness for transmission via the internet. Establishing a connection between a Virtual Private Network (VPN) tunnel terminator situated on the destination network and a VPN tunnel initiator situated on the source network, as well as vice versa, is a feasible undertaking. The VPN tunnel terminator will be located on the destination network. Once the encryption mechanism has been mutually agreed upon by both ends of the tunnel, the initiator of the tunnel encrypts the packet to guarantee its security. Upon completion of this stage, the Virtual Private Network (VPN) initiator will encapsulate the entire encrypted bundle within an Internet Protocol (IP) packet. By employing an Internet connection that solely relies on IP addresses, it is no longer imperative to transmit data utilising the identical protocol that was initially employed for its transmission.

Moreover, due to the encryption of the packet, it would be impossible for any individual to decipher the initial content. At the receiving end, the VPN tunnel terminator eliminates the IP details from the packet. Upon selecting an encryption method, the encrypted packet is transmitted to either the remote access server or the local router, where it is subsequently decrypted. This occurs subsequent to the selection of the encryption technique. Subsequently, the remote access server or the local router will transmit the IPX packet, which has been camouflaged, to the network to facilitate its delivery to the designated destination.

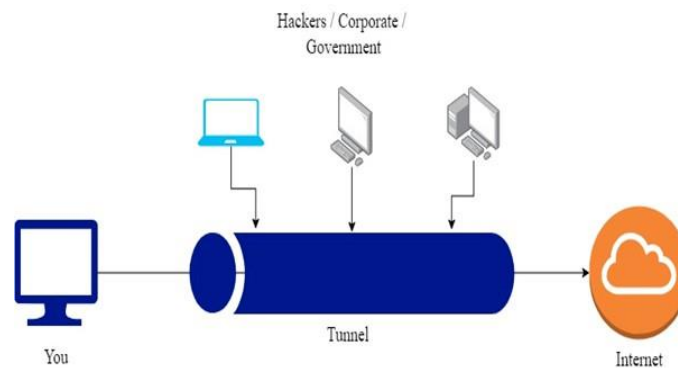


Fig. 5. VPN Working

Vpn Security

Security is a crucial and indispensable concern for businesses on a global scale. As per Gartner's analysis, organisations require a secure and reliable framework for their infrastructures to mitigate the risk of malicious activities originating from both internal and external sources. Security is a major concern for organisations worldwide. Data acquired from the remote site

- Getting Infected by malware/viruses
- Getting Intrude by phisher/hackers
- Disruption in the network that stores data

Virtual Private Network (VPN) provides a range of security measures that aid in mitigating the vulnerabilities and threats present in your network, as previously mentioned. The subsequent actions to be executed are as follows:

- A VPN protects network data transmission by authenticating and encrypting it.
- Secure VPNs feature an excessive number of tunnel, and at the end of each tunnel there are two endpoints, one for the sender and another for the receiver.

The security qualities of the tunnel are accepted and agreed upon by both the sender and the recipient:

- No outsider or other third party may make edits, modify, or otherwise affect the security features of the VPN.
- A VPN establishes a dedicated channel between two endpoints, namely the sender and the receiver. It is impossible for a third party that does not have access to the VPN to modify or change this trusted transmission channel. Changing the trusted route is the only thing that the VPN provider can do.
- An observer from the outside cannot modify, add, or remove data from a route in a VPN.

- Before a virtual private network (VPN) can be constructed, it is essential to first create the appropriate routing information and addressing information.

There is a clear definition of the VPN's address borders, which allows data transfer between two addresses in a safe and trustworthy way.

Vulnerabilities And Risks Associated With VPNs - Using a VPN makes a client node vulnerable to attacks from both within and outside the network. An attacker may attempt to take advantage of weaknesses in the client and launch an attack on the computer. The following are examples of attacks:

- Hijacking of a VPN.
- Man-in-the-middle attacks are expected.

A VPN hijacking attack involves the unauthorised acquisition of a network client machine's identity by a hacker who gains control of the VPN connection.

A type of cyber attack referred to as a man-in-the-middle attack occurs when an unauthorised computer intercepts communication between network nodes and alters the transmitted data. Modifications such as the inclusion, removal, or modification of data are among the various types of alterations that can occur.

Risks Associated With The Client - Clients may possess dual connections, one for accessing the Internet and the other for connecting to an intranet or a restricted network, contingent upon their requirements. The act of connecting a private network to the public network, commonly referred to as the Internet, may lead to the compromise and vulnerability of the private network, subjecting it to potential attacks. Regarding network security, it is feasible for a client system to be connected to a compromised system.

The Capacity To Communicate With One Another (Interoperability) - The establishment of security protocols for data transmission necessitates mutual agreement between the two interconnected systems that interface with the network. Synchronisation issues may arise between manufacturers' protocols on either end of a transmission. This has the potential to escalate the risks within the network.

Infections Caused By Viruses Or Malware - In the event of a client computer being infected with malware or a virus, it is imperative that the network be promptly shut down to prevent the entire system from being vulnerable to intrusion. The password associated with the aforementioned VPN connection is susceptible to being compromised by an unauthorised individual. The propagation of a virus or malware on a client system can potentially compromise the security of other interconnected devices within the network, thereby exposing them to potential threats. Therefore, it is imperative that the network is equipped with a reliable anti-virus system.

VPN Security Protocols - A Virtual Private Network (VPN) enables the establishment of a secure connection to end hosts or subnets that have been authenticated as members of the VPN. For a virtual private network (VPN) to achieve success, it is imperative that it satisfies the following criteria.

Authentication: The Virtual Private Network (VPN) provides data authentication services to verify the identity of the sender.

Data integrity refers to the concept of data integrity pertaining to the state of data being free from any unauthorised alterations or manipulations during its transmission.

Protection of confidentiality: The encryption of data ensures that it becomes inaccessible to other network users. The information can only be viewed by the sender and the recipient.

A Virtual Private Network (VPN) is an effective measure to thwart potential attackers from intercepting and replaying data at a later point in time.

Furthermore, the feasibility of interoperability with diverse VPN networks is attributed to the utilisation of standard-based technologies in VPNs.

Protocol In Vpn

PEER-PEER VPN - P2P Virtual Private Network (VPN) solutions facilitate involvement exclusively from peers who have established mutual trust. In order to accomplish this, it is possible to authenticate and authorise client requests through a central server, such as a connecting hub. Alternatively, individuals have the option to establish a decentralised network by exchanging cryptographic keys or passwords with their peers. The utilisation of tunnelling is a prevalent technique within the realm of network communications. This method allows for the encapsulation of a datagram utilising an alternative protocol, similar to the encapsulation of a packet with a distinct protocol using the identical method. Windows-based Virtual Private Network (VPN) connections utilise Point-to-Point Tunnelling Protocol (PPTP) packets to encapsulate and convey private network activities, including TCP/IP data, across a public network, such as the Internet. PPTP is a tunnelling protocol that employs point-to-point connections as a means of facilitating secure communication. The abbreviated form "PPTP" refers to the Point-to-Point Tunnelling Protocol. [3] The virtual private network server can be configured to use either Windows or the Remote Authentication Dial-In User Service as an authentication provider, depending on the chosen configuration. The antecedent

conditions of the configuration played a pivotal role in the determination of selecting this alternative. For a brief moment, let us assume that Windows has been designated as the authentication provider. In such instances, individuals seeking VPN connections are obligated to furnish their user credentials, which are subsequently authenticated through the customary Windows authentication protocols. Assuming successful implementation, the VPN client's user account settings and regional remote access rules authorise the connection attempt. If Windows is not chosen as the authentication provider, users' credentials for VPN connection are authenticated using conventional Windows authentication protocols.

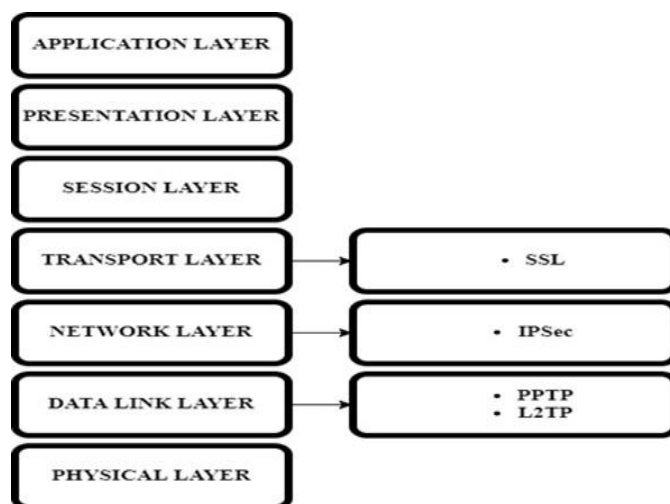


Fig. 6. Protocols of VPN in OSI Model

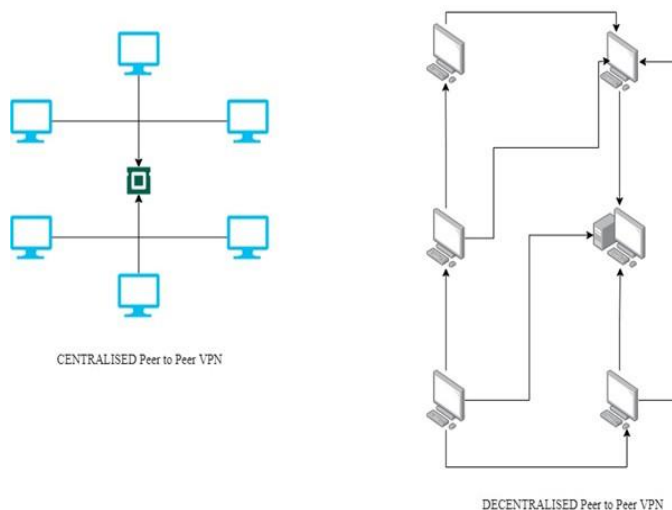


Fig. 7. Peer-to-Peer VPN (a)

MPLS VPN - Multi-Protocol Label Switching Virtual Private Networks (MPLS VPNs) are a flexible approach to network traffic transportation and routing that utilises an MPLS backbone. MPLS Virtual Private Networks leverage the benefits of MPLS in conjunction with the routing functionalities of the Border Gateway Protocol (BGP). BGP is utilised for the dissemination of routes within the provider's network backbone, whereas MPLS is employed for the transmission of packets across the provider's network backbone. [4] An MPLS VPN comprises various equipment types, as enumerated above. The networking devices utilised by customers are commonly denoted as Customer Edge (CE) routers. In general, it is common for the entity offering a particular service to possess and install the necessary equipment on the site where the service is being rendered. Furthermore, a number of service providers offer the option of renting the requisite CE equipment to their clientele for an additional charge. Provider Edge (PE) routers. The Customer Edge (CE) routers establish connectivity with the Service Provider Edge (SPE) routers in order to establish a closed circuit. The ownership of PE routers is exclusively held by the service provider. Provider (P) routers are utilised by service providers for routing purposes. The aforementioned routers are strategically located within the primary network of the service provider and are commonly denoted as "transit routers." The transmission of routing information from the CE router to the PE router can be facilitated through the utilisation of either static routes or a routing protocol such as BGP. The Provider Edge (PE) router maintains a record of the forwarding table for each site, which is commonly referred to as a Virtual Routing and Forwarding Table (VRFT) or VRF.

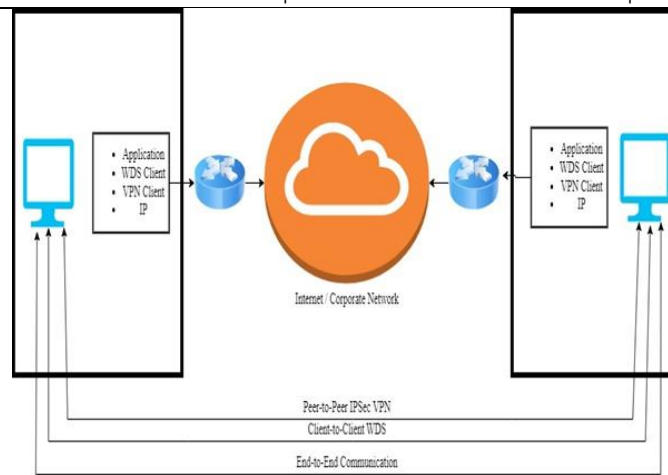


Fig. 8. Peer-to-Peer VPN (b)

INTERNET PROTOCOL SECURITY (IPSec): IPSec is re- garded as a highly comprehensive, secure, and widely ac- cessible standard, owing to its reliance on well-defined data transmission protocols. The network layer operations are un- der its responsibility. IPSec protocols have the potential to facilitate the process of cryptographic key negotiation between two communicating parties, particularly during the initial stage of the session when mutual authentication is established [1]. The IPSec network, comprising various security protocols, enables the system to effectively choose the optimal secu- rity protocols for data transmission. IPSec has the capability to secure data transmission not only between two hosts, but also between two security gateways, such as firewalls or routers. The Internet Protocol Security (IPSec) protocol facilitates the secure transfer of data between senders and receivers by providing user authentication, data encryption, and data integrity. The establishment of a secure connection and transportation of data is facilitated by the utilisation of three fundamental protocols, specifically the Authentication header, the Encapsulated Security Payload, and the Internet Key Exchange.

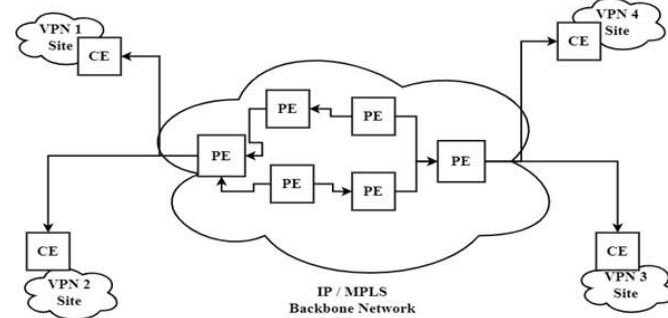


Fig. 9. MPLS VPN

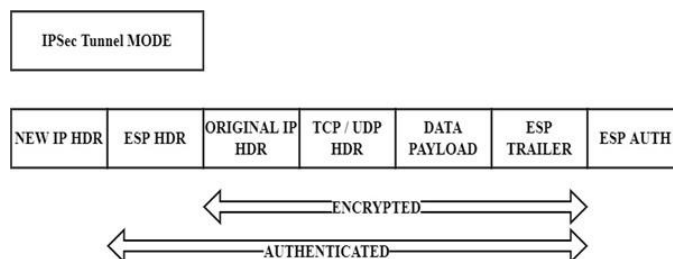


Fig. 10. IPSec VPN Header

Authentication Header (AH): Authentication The header pro- tocol assumes responsibility for both verifying the authenticity of source nodes and maintaining the integrity of the data. Si- multaneously, it performs both of these tasks. The system lacks the ability to perform data encryption. The inclusion of AH is a standard feature in the compressed configuration of every IP packet. The Authentication Header (AH) encompasses various details such as the hashed data, sequence number, security parameter index, and other pertinent information.

Encapsulated Security Payload (ESP): To provide greater clar- ity, The Encapsulated Security protocol provides three crucial services, namely data confidentiality, data consistency, and identification of the data source. To ensure the preservation of user confidentiality and the protection of your data, symmetric algorithms are used to encrypt all information. It is imperative that the encryption algorithm employed by the sender and the recipient be identical for mutual communication.

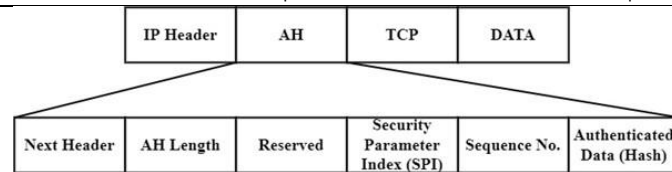


Fig. 11. Authentication Header

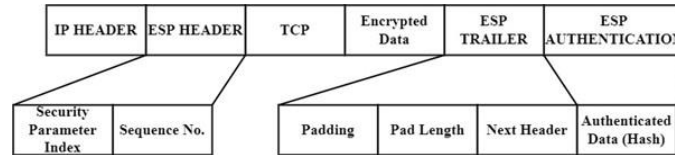


Fig. 12. ESP Header

All security protocols can operate in two modes at the same time. They are as follows:

- Tunnel Mode
- Mode of Transportation

The operations performed on a network encompass a specific mode of operation referred to as tunnel mode, which is alternatively recognized as the end-to-end mode of operation. In the process of linking two locations within a virtual private network (VPN), a communication pathway is established through a shared network, commonly referred to as a tunnel. In the context of networking, the utilization of tunnel mode involves the incorporation of both communal virtual private network (VPN) nodes and shared network infrastructure nodes at the endpoints of the tunnel. The utilization of the tunnel mode provides a safeguard for confidential data. Apart from the ESP header and trailer, the data packet comprises encrypted data, an outdated IP header, a current IP header, an outdated IP authentication header, and a current IP authentication header. The updated IP header now incorporates the endpoint address of the tunnel. After decryption of the encrypted data packet by the tunnel point and subsequent identification of the destination address, the initial data packet is directed towards its intended destination address through the network. Subsequent to the identification of the intended destination address through the deciphered data within the encrypted packet, this event takes place.

Various terminologies are used to describe the mode of operation for transportation, one of which is the host-to-host mode of operation. The data packet comprises various constituents, such as the ESP header and trailer, ESP authentication, and the IP header, among other elements. The IP header lacks encryption measures for protection. Consequently, there exists a potential for adversaries to intercept the address through this means. Due to the accessibility of header information, it is feasible for attackers to analyze the transmitted data traffic.

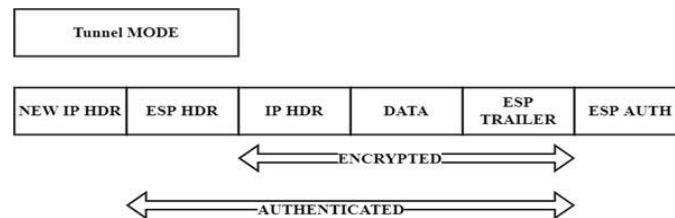


Fig. 13. Tunnel Mode Header

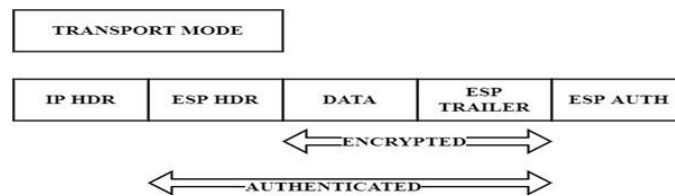


Fig. 14. Transport Mode Header

POINT TO POINT TUNNEL PROTOCOL (PPTP): This protocol functions at the level two of the OSI model and is a layer two protocol that is constructed over the Point to Point Protocol (PPP). PPTP facilitates the connection of remote clients to the target network by establishing a virtual network for each client on the network. For the PPTP tunnel to operate effectively, it is essential that the PPTP call control and management message be conveyed through the PPTP control connection [3]. The PPTP protocol enables the tunneling of a PPP session over an IP network, utilizing a protocol distinct from TCP/IP. PPTP employs a variety of authentication mechanisms. The aforementioned protocols are Extensible Authentication Protocol (EAP), Microsoft Challenge Handshake Authentication Protocol (MCHAP), Shiva Password Authentication Protocol (SPAP), and Password Authentication Protocol (PAP). The PPTP tunnelling protocol involves the repeated encapsulation of data

packets, which leads to an increase in the size of the resulting packet. The Generic Routing Encapsulation (GRE) protocol is utilized by the Point-to-Point Tunneling Protocol (PPTP) to encapsulate the Point-to-Point Protocol (PPP) data frames prior to transmitting them over a public network, such as the Internet, to the intended destination. Furthermore, aside from furnishing data. In addition to encapsulation, the GRE protocol offers flow control and congestion management mechanisms for the transmission of data. The data frames of the PPP protocol are encrypted within a protective enclosure. The enclosed and encrypted data frame is augmented with an IP header to provide protection against unauthorized interception. The IP header contains the source and destination IP addresses. Once the PPTP data packet arrives at the PPTP server, it is eliminated from the network. The process of deciphering the Point-to-Point Protocol (PPP) and eliminating the Internet Protocol (IP), Generic Routing Encapsulation (GRE), and PPP headers from the transmitted data packet.



Fig. 15. PPTP Header

LAYER 2 TUNNELING PROTOCOL (L2TP): L2TP serves as a means of encapsulating data for transmission between communication nodes across various protocols, including Asynchronous Transfer Mode, Frame Relay, and X.25 networks. Moreover, L2TP is implemented at the second layer of the OSI reference model. It is possible to establish numerous connections through a solitary tunnel. The Layer 2 tunneling protocol is capable of transmitting non-IP protocols via an IP network by utilizing PPP frames to encode data. The authentication procedures utilized in L2TP connections are identical to those employed in PPP connections, including EAP, CHAP, and MSCHAP. The process of tunneling over L2TP involves the utilization of multiple layers of encapsulation and encryption. The L2TP and PPP headers provide a safeguard for the PPP data against interception by the recipient's computer. The L2TP packet is encapsulated within a UDP header prior to transmission over the network. The ultimate data unit is encompassed by an Internet Protocol header that comprises the originating and terminating Internet Protocol addresses of the Virtual Private Network client and Virtual Private Network server, along with the timestamp. L2TP protocol does not reveal information surreptitiously. Consequently, L2TP is frequently employed in conjunction with IPsec and denoted as L2TP/IPsec. The utilization of L2TP in tandem with IPsec results in the utilization of the security services provided by IPsec, namely AH and ESP. The L2TP controls and data are presented to the IPsec system as a unified sequence of uniform IP packets.

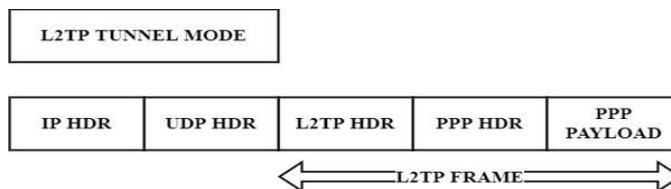


Fig. 16. L2TP Header

KEY EXCHANGE AND MANAGEMENT - To enable key management for VPNs over public networks, IPsec supports two essential management methods. They are as follows:

- Manual Key Management.
- Automated Key Management.

Table II Characteristics of VPN Protocol

VPN Protocol	Speed	Encryption	Streaming	Stability
OpenVPN	Fast	Very Good	Good	Good
IPsec/IKEv2	Fast	Good	Good	Very Good
Wireguard	Very Fast	Very Good	Good	Very Good
SSTP	Medium	Good	Medium	Medium
L2TP	Medium	Medium	Poor	Good
PPTP	Fast	Poor	Poor	Good

Prior to establishing a connection between the two entities, manual key management necessitates that the sender and receiver engage in the exchange of secret keys. Only the sender and the recipient possess knowledge of the values of the secret keys and security associations that have been established. In the context of a limited and unchanging network infrastructure, the

implementation of key management protocols may be deemed suitable. Before initiating any specific data transmission, the involved parties engage in the exchange of confidential keys and mutually inform each other of the communication nodes. This stipulation renders the network incapable of dynamic scaling or reconfiguration. The compromise of secret keys by an external entity, such as an attacker, could potentially compromise the security of the network. The most notable limitation of this approach is its potential to render the network susceptible to security breaches.

The establishment and management of confidential keys between communicating network nodes is accomplished through the utilization of IPSec's customary protocol. The term commonly used in media circles to denote the process is Internet Key Exchange (IKE).

Compared to the traditional approach of manual key management, a network utilizing this type of key management has the advantage of being adaptable and capable of being expanded as required. IKE is accountable for the subsequent obligations.

- Users' Identification and Authentication.
- Session Negotiation between the people involved in the communication.
- For data transfer, a key exchange protocol is used.
- IPSec tunnel negotiation and setup are covered in this section.

IKE's most crucial role is to execute authentication on behalf of the user. It authenticates the communicating nodes to each other by using one of the techniques listed in the next section.

- IKE uses a shared key - a hashing method that assures that only the nodes that have the key may transmit data packets.
- IKE's Digital Signature Standard uses public-key digital signature encryption to confirm the identity of the nodes participating in the data transmission.
- In order to guarantee that the negotiation between the two nodes can only take place if each node has the right private key, which is only feasible if each node has the right private key, it uses encryption techniques.

The IKE protocol confers upon the communicating nodes the capacity to engage in negotiation pertaining to the authentication mechanism, exchange algorithm, and encryption technique to be employed during the session. The negotiation has the potential to occur at any point during the session. The culmination of this phase occurs prior to the effective transmission of information among the nodes. The IKE protocol employs negotiated key exchange as a means of ensuring a secure exchange of information between both the sender and receiver. A novel secret key is generated and employed to safeguard the data exchange during each individual session of data transaction.

Upon completion of the negotiation of a secure method of information transfer, IKE initiates the negotiation of an IPSec tunnel connection. The Internet Key Exchange (IKE) protocol generates a novel confidential key that is subsequently employed by the Internet Protocol Security (IPSec) tunnel. The techniques employed in this tunnel for the purposes of authentication and encryption are also addressed. The configuration of IPSec tunnels for LAN-to-LAN connections is recommended to be performed through the VPN Group section, while the Tunnel Partner section is suggested for VPN Client connections.

Related Work On Vpn

Various techniques have been suggested by scholars to categorize network traffic as either Virtual Private Network (VPN) or non-VPN. Several techniques currently exist in the field, including Long-Short Term Memory (LSTM), Data Packet Inspection (DPI), Pattern Recognition, Classical Port-Based approach, Payload based classification, and Machine Learning (ML). Scholars have proposed diverse computational methodologies as plausible approaches for carrying out a precise inquiry of network traffic data. The identification of network breaches remains a significant area of research in the field of network security, owing to the dynamic nature of network traffic patterns. The relevance of Machine Learning techniques in addressing the aforementioned issue can be attributed to their ability to efficiently handle data, automate processes, and have a wide range of applications. Figure 16 illustrates the various categories of Machine Learning. Figure 17 depicts the Venn Diagram representing the field of Artificial Intelligence.

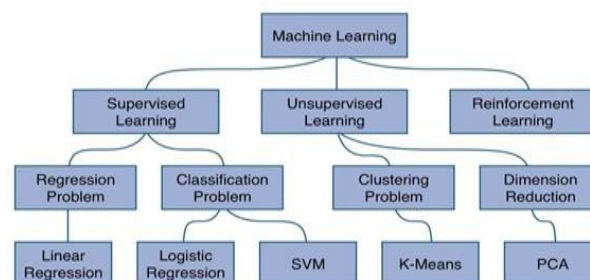


Fig. 17. Types of Machine Learning

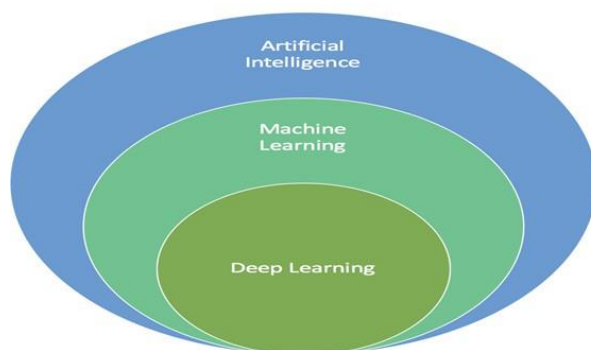


Fig. 18. Venn Diagram of Artificial Intelligence

II. Brief Review of the Work Done in the Field

Numerous scholars have devised intelligent methods of categorizing standard and virtual private network (VPN) traffic. The current study centers on machine learning-based approaches for identifying and categorizing regular traffic and VPN traffic. This section provides a summary of the research contributions in this area and highlights the unresolved issues and challenges that require further investigation by researchers. In 2006, Suheyli Ikiz and Y.M.Erten [1] The effects of employing Virtual Private Networks (VPNs) on the throughput of wireless Local Area Networks (LANs) were discussed. The researchers established a testbed and utilized empirical data obtained from conducted tests to derive their conclusions. The study conducted by the authors involved the implementation of an IEEE 802.11g wireless LAN, wherein they analyzed and compared the throughput statistics obtained from the utilization of IPSec in the said network with the computed data. The present study conducted a comparison utilizing an IEEE 802.11g wireless local area network. The research findings indicate that network performance is influenced by significant factors such as the number of simultaneous VPN connections, inter-frame time between packets, and packet size.

In 2012, R. Antonello et al. [2] The author provided a comprehensive review of the tools and methodologies necessary for the development of contemporary Deep Packet Inspection (DPI) systems. The technical background information and analysis of the current research in the field of optimizing DPI engines for commodity platforms were both presented. Subsequently, an analysis was conducted on the existing obstacles encountered in the field of research, followed by recommendations for the development of efficient DPI systems.

In 2016, Saman Fegghi et al. [3], The author has developed a method to breach encrypted web traffic using exclusively the timing data of uplink packets. Consequently, the traditional techniques of packet padding are rendered futile in countering this assault. In contrast to prior endeavors, this particular timing-based assault does not necessitate awareness of the initiation or termination of web requests, thereby rendering it effective against traffic streams. The study demonstrates the effectiveness of the attack on both wired and wireless traffic, achieving an average success rate exceeding 90%. The aforementioned temporal-based attack, apart from its inherent intrigue, exposes vulnerabilities in current security measures and highlights aspects that VPN developers ought to prioritize. In the literature, S. Bagui et al. [4] In 2017, a technique was proposed and developed to differentiate between network traffic that utilizes Virtual Private Networks (VPNs) and those that do not, based on temporal properties. This study compares six distinct models of categorization. The Random Forest (RF) and Gradient Boosting Tree (GBT) classifiers are recommended over logistic regression, support vector machine, Naive Bayes, k-nearest neighbor, and ensemble approaches due to their high accuracy and minimal overfitting.

Lulu Guo et al. [5], in 2019, The proposed research aims to attain the experiment objectives through the utilization of models that employ convolutional neural network (CNN) and convolutional auto-encoding (CAE) techniques to transform traffic samples into session pictures. The CAE-based technique leverages the unsupervised nature of CAE to extract latent features, enabling automatic identification of nonlinear relationships between the input and output variables. The proposed methodology combines the unsupervised characteristic features of Convolutional Autoencoder (CAE) with the advantages of Multi-Layer Perceptron (MLP) in data dimensionality reduction and supervised classification learning techniques, with the aim of achieving a dependable identification of Virtual Private Network (VPN) encrypted traffic.

In 2019, Y.Zhang et al. [6] The study initially focused on several widely utilized open-source secure proxy protocols and conducted a static analysis of their vulnerabilities. Subsequently, Deep Learning (DL) is employed to train the entirety of the interconnected network traffic, and the results demonstrate that all secure proxy traffic can be accurately distinguished with a high degree of precision.

In 2020, Shane Miller et al. [7] This study aims to suggest computational methodologies for addressing the current limitations in detecting Virtual Private Network (VPN) data. The study employed a Multi-Layer Perceptron Neural Network (MLPNN) to construct a predictive model aimed at identifying Virtual Private Network (VPN) usage. The model was developed by analyzing flow statistics data extracted from the Transmission Control Protocol (TCP) header of network packets that were

intercepted. The results of the validation testing indicate that the models provided were able to reasonably and accurately categorize network traffic as either direct, originating directly from a user's device, or indirect, utilizing location masking capabilities and VPN identity.

In 2020, P. Gao et al. [8] Six distinct categories of VPN traffic were analyzed. A framework was developed by the researchers to classify Virtual Private Network (VPN) traffic by utilizing Payload Length Sequence as the basis. Machine learning techniques are employed to construct classifiers for VPN traffic using Sample Entropy Fingerprint (SEF) and PLS (Payload Length Sequence) as distinct features for characterizing VPN traffic. In comparison to Deep Packet Inspection (DPI), SEF, and PLS. The findings indicate that the classifier based on Partial Least Squares (PLS) is capable of effectively categorizing Virtual Private Network (VPN) data, including VPN traffic that has been concealed.

In 2020, Raoul Nigmatullin et al. [9] The proposed technique, known as Differentiation of Sliding Rescaled Ranges (DSRR), is a novel traffic preprocessing approach that leverages the theoretical framework developed by H.E. Hurst. The researchers utilized a proposed methodology to categorize both encrypted and unencrypted traffic on the widely recognized ISCXP2016 dataset. The researchers employed DSRR methodology to analyze flow-based characteristics and utilized basic machine learning models to address the task of distinguishing between VPN and non-VPN traffic. The DSRR and Random Forest (RF) models were found to achieve precision and recall scores of 0.971 and 0.969, respectively, according to the researchers' findings. In contrast to the precision of 0.93 achieved by the Neural Network method utilizing 2D-CNN, the utilization of statistical feature analysis enhances this outcome to 0.976.

In 2020, Soo-Yeon Ji et al. [10] A comprehensive analysis was conducted on the existing literature pertaining to visualization techniques used for the analysis of network traffic data. The review has identified four fundamental techniques that are crucial for the development of a satisfactory Network Traffic (NT) visualization system. These techniques include pixel-based visualization, graph representation, data filtration, data transformation, and coordinated multi-views. The researchers developed multiple prototype visualizations and conducted an analysis of their applicability, data preprocessing requirements, network pattern comprehensibility, and anomalous network event identification to evaluate the efficacy of four distinct visualization techniques.

In 2016, Gerard Draper-Gil et al. [15] The present study examined the efficacy of flow-based temporal attributes in identifying Virtual Private Network (VPN) traffic and categorizing encrypted communication into discrete groups based on the nature of the traffic, such as web browsing, media streaming, and the like. Two widely recognized machine learning algorithms, namely C4.5 and KNN, are utilized to evaluate the precision of features. The findings demonstrate a high level of precision and efficiency, indicating that temporal characteristics serve as effective discriminators for the categorization of encrypted network traffic.

Noteworthy Contributions in the Field

So far, several studies have been carried out in the Field of VPN traffic detection. The following individuals have made significant contributions to the Field:

Vladimir A. Muluikha et al. [11], 2020, A specimen of an intelligent system has been developed for advanced analysis of encrypted communications. The system is based on models and software that were developed by Peter the Great at St. Petersburg Polytechnic University. This study examines the efficacy of identifying application detection and user activity within encrypted Secure Sockets Layer sessions in Virtual Private Network connections. The Map-Reduction Paradigm has been integrated, facilitating an in-depth analysis of Network traffic. The article presents empirical research results regarding software that has the ability to categorize encrypted communications. The Random Forest technique is employed for the purpose of discriminating VPN connections, while the Simple Bayesian Classifier approach is utilized for the classification of SSL traffic.

In 2021, F. U. Islam et al. [12] A novel approach was proposed for deciphering encoded network data and detecting obscured and untraceable network communication. The proposed methodology for identification employs deep learning techniques, which are highly coveted, to discern unidentified network traffic and extract Voice over IP (VoIP) and Non-VoIP traffic flows from encrypted communication flows. The traffic obtained was categorized into four distinct groups, namely TOR VoIP, TOR Non-VoIP, VPN VoIP, and VPN Non-VoIP, at the conclusion of the study. The experimental findings indicate that the identification engine exhibits a high degree of resilience against the traffic generated by virtual private networks (VPNs) and the TOR network.

Bei Lu, Nurbol Luktaran, et al. [13] In 2021, an Inception-LSTM (ICLSTM) approach has been proposed as a traffic classification strategy to identify encrypted traffic services. The essential characteristics and traffic have been effectively categorized. In order to mitigate the problem of class disparity, distinct weights are computed for individual segments during the training process to enhance symmetry across various segments of encrypted traffic. This approach aims to promote a more equitable and balanced detection efficacy.

III. Critical Analysis and Discussion

A. Identified Trends and Patterns: The increasing usage and popularity of VPNs due to their cost-effectiveness and security features. There is a trend towards utilizing VPNs to overcome limitations of public networks in transmitting sensitive or non-IP data securely. The paper implicitly advocates for the use of encryption and tunnelling as core best practices for secure data transfer over public networks. It also emphasizes the necessity of mutual authentication between VPN clients and servers.

B. Research Gaps:

- 1) **Traffic Classification Challenges:** The paper explicitly states that "The task of analysing and identifying encrypted network traffic associated with specific applications and pro- tocol con- figurations poses a significant challenge for network adminis- trators". This highlights a critical gap in distinguish- ing traffic within encrypted tunnels.
- 2) **Efficacy of Visualization Techniques:** The paper points out that "the extent to which visualisation techniques are efficacious in the analysis of network traffic data has not been extensively investigated", indicating a research gap in visual analytics for network security.

Table Iii Summary

TITLE	ANALYSIS	CHALLENGES
Effects of VPN on WLAN Throughput	Analyzed throughput with IPSec	Simultaneous connections, inter-frame time, packet size
Optimizing DPI Systems	Identified performance bottlenecks	Efficient implementation on commodity platforms
Timing-based Attack on Encrypted Web Traffic	90% success on both wired/wireless	Padding ineffective; attacks don't require session boundaries
VPN vs. Non-VPN Traffic Classification	Compared six models	Overfitting, feature selection
CNN + CAE for VPN Detection	CNN and CAE performance evaluated	Capturing nonlinear features, training complexity
DL for Proxy Protocol Vulnerability	Accurate classification	Proxy protocol vulnerabilities
MLPNN for VPN Detection	Distinguish direct vs. indirect traffic	VPN usage classification accuracy
VPN Classification via SEF & PLS	Compared SEF, PLS, DPI	Hidden VPN detection
DSRR Traffic Preprocessing	Compared with CNN, RF	Improve precision with statistical analysis
Visualization for Network Traffic	Analysis on 4 techniques	Anomaly detection, pattern comprehension
Flow-Based Temporal Classification	High efficiency in type classification	Differentiating encrypted service types
Encrypted Session Analysis System	MapReduce + ML tools	Identifying apps and user activity in encrypted traffic
Deep Learning for Obscured Traffic	TOR & VPN traffic categorized into 4 classes	Obscured & trace-less communication
Inception-LSTM for Encrypted Services	Balanced class detection using segment weights	Class imbalance in encrypted traffic

- 3) **Standardization for Interoperability :** The "underdevel- oped nature of the standards" leading to a "potential lack of interoperability among various VPN technologies" suggests a need for further research and development in this area

C. **Challenges and Open Issues** Based on the provided paper, several challenges and open issues in the domain of Virtual Private Networks and network security are identified:

- 1) **Detecting Obfuscated Traffic:** Network managers face a significant challenge in analyzing and identifying encrypted network traffic, as users employ diverse encryption techniques to hide the true intent of their communications.
- 2) **Performance Limitations:** VPN connections exhibit suboptimal levels of performance in terms of speed and responsiveness, which can hinder user experience.
- 3) **Public Network Security Risks:** Since VPN connections are established over public networks, a comprehensive understanding of network security issues and necessary precautions is imperative before deployment.
- 4) **Internet Scalability Impact:** The stability of a VPN connection is heavily influenced by the scalability of the Internet, which is often beyond an enterprise's control.
- 5) **Interoperability Issues:** The underdeveloped standards for VPN technologies can lead to a lack of interoperability among various VPN solutions.
- 6) **Technical Difficulties:** Users may experience technical difficulties arising from malfunctioning equipment and slug- gish internet connections.

7) **Verification of Dubious Actions:** Despite the development of computational algorithms for identifying unforeseen intrusions, verifying suspicious activities and identifying their unique features remains a significant challenge.

D. Future Research Directions Drawing from the challenges and gaps identified in the paper, potential future research directions include

1) **Enhanced Encrypted Traffic Classification:** Further research is needed to develop more sophisticated techniques and computational algorithms capable of analyzing and identifying encrypted network traffic, particularly focusing on specific applications and protocol configurations within the encrypted tunnels. This would involve moving beyond basic detection of encryption to understanding the content or nature of the communication.

2) **Advanced Visualization Techniques:** Investigate and evaluate the effectiveness of visualization techniques for network traffic data analysis to enhance users' visual comprehension of data and aid in validating suspicious activities.

3) **Improved VPN Standards for Interoperability:** Research and development efforts should focus on creating more robust and widely adopted standards for VPN technologies to ensure better interoperability among different solutions and vendors.

4) **Optimizing VPN Performance:** Explore novel methods to improve the speed and responsiveness of VPN connections, mitigating the current suboptimal performance issues.

5) **Adaptive Security Measures:** Develop VPN solutions with more adaptive security measures that can respond to evolving threats and new obfuscation techniques, reducing susceptibility to unauthorized access.

IV. Conclusion

To summarize, the reviewed studies have made significant contributions to the identification and categorization of standard and virtual private network (VPN) traffic using machine learning-based approaches. These investigations have explored various techniques such as empirical analysis, deep packet inspection systems, timing-based attacks, convolutional neural networks, flow-based temporal attributes, and payload length sequence analysis.

The studies have demonstrated the impact of factors such as the number of simultaneous VPN connections, inter-frame time between packets, packet size, and timing data in influencing network performance and identifying VPN traffic. They have also highlighted the vulnerabilities in secure proxy protocols and the need for improved detection and classification of VPN usage.

The studies have showcased the effectiveness of different techniques and methodologies, including empirical analysis, deep packet inspection (DPI) systems, timing-based attacks, temporal properties, convolutional neural networks (CNN), convolutional auto-encoding (CAE), deep learning (DL), multi-layer perceptron neural networks (MLPNN), payload length sequence (PLS), and flow-based temporal attributes. These approaches have demonstrated promising results in accurately classifying VPN traffic, even in the presence of encryption and concealment techniques.

Machine learning algorithms, including Random Forest, Gradient Boosting Tree, Multi-Layer Perceptron Neural Network (MLPNN), Partial Least Squares (PLS), Differentiation of Sliding Rescaled Ranges (DSRR), and Inception-LSTM (ICLSTM), have been employed to develop effective classifiers for distinguishing VPN traffic from regular traffic. These classifiers have shown high accuracy and minimal overfitting, enhancing the capability to detect and categorize VPN traffic. Furthermore, researchers have addressed the challenges posed by encrypted and concealed VPN traffic, providing insights into breaching encryption using timing data, analyzing temporal properties, and developing techniques for classifying concealed VPN traffic.

Despite the progress made in this field, there are still unresolved issues and challenges that require further investigation. Enhancing the efficiency of deep packet inspection systems, addressing vulnerabilities in secure proxy protocols, improving the detection of VPN usage, and developing techniques for accurately classifying concealed VPN traffic are important areas that require continued research.

Overall, these studies contribute to the understanding of machine learning-based approaches for identifying and categorizing VPN traffic, providing valuable insights for network security, traffic management, and privacy protection. Further advancements in this field will continue to play a crucial role in addressing emerging challenges in the ever-evolving landscape of network communications.

Future research should focus on addressing these challenges and exploring innovative approaches to improve the accuracy and efficiency of VPN traffic identification and categorization. By continuing to advance machine learning techniques, incorporating new features and datasets, and considering real-world network scenarios, researchers can contribute to the development of robust and reliable methods for handling VPN traffic, ultimately improving network security and performance.

References

1. Ikea, S., & Erten, Y. M., "Throughput Analysis of UDP and VPN Traffic in 802.11g Networks," Lecture Notes in Computer Science, (2006), pp.474–482.
2. Antonello, R., Fernandes, S., Kamienski, C., Sadok, D., Kelner, J., Go'dor, I., . . . Westholm, T., "Deep packet inspection tools and techniques in commodity platforms: Challenges and Trends," Journal of Network and Com-

- puter Applications, (2012), 35(6), pp.1863–1878. DOI: 10.1016/j.jnca.2012.07.010.
3. S. Feghhi and D. J. Leith, "A Web Traffic Analysis Attack Using Only Timing Information," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 8, pp. 1747- 1759, Aug. 2016, DOI: 10.1109/TIFS.2016.2551203.
4. S. Bagui, X. Fang, E. Kalaimannan, S. C. Bagui &
5. J. Sheehan, "Comparison of machine-learning algorithms for classification of VPN network traffic flow using time-related features" in Journal of Cyber Security Technology, (2017), DOI: 10.1080/23742917.2017.1321891.
6. L. Guo, Q.Wu, S. Liu, M. Duan, H. Li, J. Sun, "Deep learning-based real-time VPN encrypted traffic identification methods," in Journal of Real-Time Image Processing, (2019), DOI: 10.1007/s11554-019-00930-6
7. Zhang, Y., Chen, J., Chen, K., Xu, R., Teh, J., & Zhang, S., "Network traffic identification of several open-source secure proxy protocols," International Journal of Network Manage- ment. (2019) DOI:10.1002/nem.2090.
8. Miller, S., Curran, K., & Lunney, T., "Detection of VPN Traffic Using Machine Learning." International Journal of Wireless Networks and Broadband Technologies, (2020), 9(2), pp.60–80. DOI:10.4018/ijwnbt.2020070104.
9. P. Gao, G. Li, Y. Shi, and Y. Wang, "VPN Traf- fic Classification Based on Payload Length Sequence," 2020 International Conference on Networking and Net- work Applications (NaNA), 2020, pp. 241-247, DOI: 10.1109/NaNA51271.2020.00048.
10. R. Nigmatullin, A. Ivchenko, and S. Dorokhin, "Differ- entiation of Sliding Rescaled Ranges: New Approach to En- crypted and VPN Traffic Detection," 2020 International Con- ference Engineering and Telecommunication (En&T), 2020, pp. 1-5, DOI: 10.1109/EnT50437.2020.9431285.
11. Ji, S.-Y., Jeong, B.-K., & Jeong, D. H., "Evaluating visu- alization approaches to detect abnormal activities in network traffic data," International Journal of Information Security, (2020), 20(3), pp. 331–345. DOI:10.1007/s10207-020-00504-9.
12. V. A. Muliukha, L. U. Laboshin, A. A. Lukashin, and N. V. Nashivochnikov, "Analysis and Classification of Encrypted Network Traffic Using Machine Learning," 2020 XXIII International Conference on Soft Comput- ing and Measurements (SCM), 2020, pp. 194-197, DOI: 10.1109/SCM50615.2020.9198811.
13. F. U. Islam, G. Liu, J. Zhai, and W. Liu, "VoIP Traffic Detection in Tunneled and Anonymous Networks Using Deep Learning," in IEEE Access, vol. 9, pp. 59783-59799, 2021, DOI: 10.1109/ACCESS.2021.3073967.
14. Lu, B., Luktarhan, N., Ding, C., & Zhang, W., "ICLSTM: Encrypted Traffic Service Identification Based on Inception- LSTM Neural Network," Symmetry, (2021), 13(6), 1080. pp.1- DOI:10.3390/sym13061080.
15. Lee, J., & Lee, H., "An SSH predictive model using machine learning with web proxy session logs," International Journal of Information Security, (2021). DOI:10.1007/s10207- 021-00555-6.
16. A. A. Jaha, F. B. Shatwan and M. Ashibani, "Proper Virtual Private Network (VPN) Solution," 2008 The SecondInternational Conference on Next Generation Mobile Appli- cations, Services, and Technologies, 2008, pp. 309- 314, doi: 10.1109/NGMAST.2008.18.