THE ASIAN BULLETIN OF BIG DATA MANAGEMENT

Vol.4. Issue4 (2024)

https://doi.org/ 10.62019/abbdm.v4i4.287

Enhanced Classification of Networks Encrypted Traffic: A Conceptual Analysis of Security Assessments, Implementation, Trends and Future Directions

Irfan Farooq, Syed Aale Ahmed*, Asfar Ali, Muhammad Ali Warraich, Muhammad Aqeel, Hamayun Khan

Chronicle

Article history

Received: Oct 12, 2024
Received in the revised format: Oct 29, 2024
Accepted: December 11, 2024
Available online: December 20, 2024

Irfan Farooq, Syed Aale Ahmed*, Asfar Ali, Muhammad Aqeel, and Hamayun Khan are currently affiliated with Faculty of Computer Science & IT Superior University Lahore, Pakistan.
Email: SU92-MSCSW-S24-004@superior.edu.pk
Email: SU92-MSCSW-S24-012@superior.edu.
Email: asfarali761@gmail.com
Email: aqeel@superior.edu.pk
Email: hamayun.khan@superior.edu.pk

Muhammad Ali Warraich is currently affiliated with Dice Technologies
Email: muhammadwarraich007@gmail.com

Corresponding Author*

Abstract

Encryption is a fundamental security measure to safeguard data during transmission to ensure confidentiality while at the same time posing a great challenge for traditional packet and traffic inspection. With the widespread use of encrypted data transport, network traffic encryption is becoming a standard nowadays. This presents a challenge for traffic measurement, especially for analysis and anomaly detection methods, which are dependent on the type of network traffic. In this paper, we survey existing approaches for classification and analysis of encrypted trafficIn response to the proliferation of diverse network traffic patterns from IOT devices, websites, and mobile applications, understanding and classifying encrypted traffic are crucial for network administrators, cybersecurity professionals, and policy enforcement entities. This paper presents a comprehensive exploration of recent advancements in numerous virtual private network and machine-learning-driven encrypted security protocols, that examines their critical role in modern networking and the protection of sensitive data across untrusted networks its traffic analysis and classification. We present the overall procedure and provide a detailed explanation of utilizing machine learning in analyzing and classifying encrypted network traffic. As VPN technologies have evolved over time, and today, they are essential in ensuring secure communications for both personal and enterprise use. This study also delves into various VPN protocols such as PPTP, L2TP/IPsec, OpenVPN, IKEv2/IPsec, and the newer WireGuard, evaluating their security features, strengths, and weaknesses in different network environments and reviewed state-of-the-art techniques and methodologies in traffic analysis. Our aim is to provide insights into current practices and future directions in encrypted traffic analysis and classification, that focusing on the integration of AI for enhanced VPN security and the adaptation of VPN protocols to a post-quantum world especially machine-learning-based analysis.

Keywords: VPN, PPTP, L2TP/IPSec, Open VPN, IKE/IPSec, WireGuard, Encryption, machine learning; traffic classification; device fingerprinting

INTRODUCTION

Federated First of all it is a network, that is, it delivers connection to pass elements and data between the different buyers who belong to the VPN. Secondly it is private, that is, it has all the features of a private network the principle of its work implies this. Therefore, it is logical to ask "what defines a private network. Private network is

typically deployed to maintain a secure environment where only a number of selected users have been granted access to a whole range of network-related services & tools [1, 2]. Teletraffic that originate and terminate within a private network transverse only nodes within the private network domain. Besides that, there is traffic isolation. It means that, the traffic associated with this private network does interplay with other traffic unrelated or unrelated to the private network. The last quality that is characteristic of VPN is that it should be virtual in nature [3, 4]. A virtual topology is overlaid on a pre-existing physical telecommunication infrastructure. A Virtual Private Network (VPN) is additional private network that is extended through to the links in shared or even public telecommunication network for instance the Internet. A VPN allows you to transmit data from one or more computers in one internetwork over shared or public internetworks while implementing the characteristics of communication that happen directly between two nodes. The process by which virtual private network is set up and developed is called virtual private networking [5, 6].

To resemble the point-to-point link in [6], data is encapsulated or wrapped with a header that shows a routine information sending it through the shared or public internetworks to its destination point. In order to mimic private link, data transmitted is encrypted for the purpose of security. When the packets are captured on the shared or the public network then they cannot be understood without the keys on encryptions. The link in which the private data is encapsulated or encrypted is called virtual private network (VPN) connection. A VPN connection enables a user who is at home or on the road to assume a secure connection to a server on a corporate Internet via the Internet routing structures [7, 8].

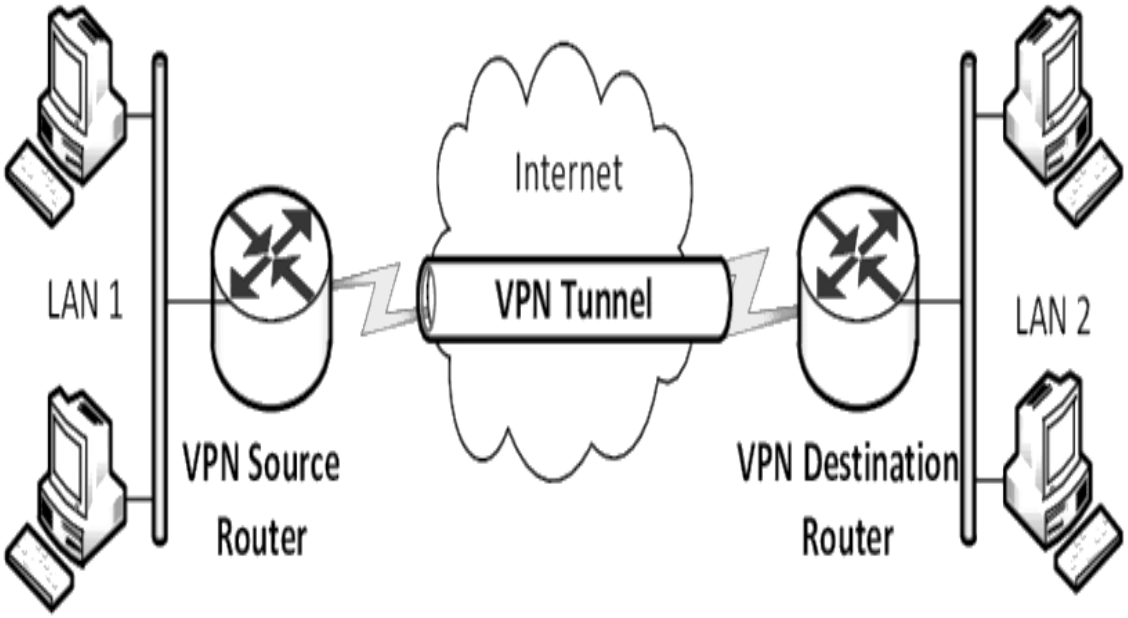

Figure 1.

Virtual private network Tunnelling from LAN1-LAN2 [9]

From the user's point of view, the VPN connection appears to be a dedicated connection between the user and its computer and the corporate server. The fact that the internetworks are intermediate is immaterial to the user since the data looks as if is being transmitted through a dedicated private circuit. VPN connection also enables a corporation to connect with branch offices or with another company over an open internetwork say like the world wide web and still have a secure line of communication. VPN connection in Internet logically can be looked as a WAN link between the sites [10]. As in both these cases, the internetwork connection looks like a private network communication to the user while in fact the internetwork is public and hence the name virtual private network [11].

Table 1: Comparative Analysis of Security Protocols [12]

Protocols/Features	PPTP	L2TP/IPSec	OpenVPN
Encryption	MPPE protocol for data encryption along with RC4 cipher	IPSec along with 3DES/AES	SSL with AES and Blowfish
Key length	128 bits	256 bits	160 bits, 256 bits
Speed	Fast	Requires resources for data encapsulation	Fast
Reliability and scalability	Very stable	Reliable for NAT supported devices	Most reliable even on unstable network
Privacy and security	Inefficient	Highest security	Highest. Digital certificates

A virtual private network (VPN) connection is a secure method of transmitting private data through a dedicated private circuit. It encapsulates or wraps data with a header, allowing it to be understood by the user. VPNs allow users to connect securely to corporate servers over the internet, despite the intermediate internetworks. They also allow corporations to connect with branch offices or other companies over open networks, creating a WAN link between sites.

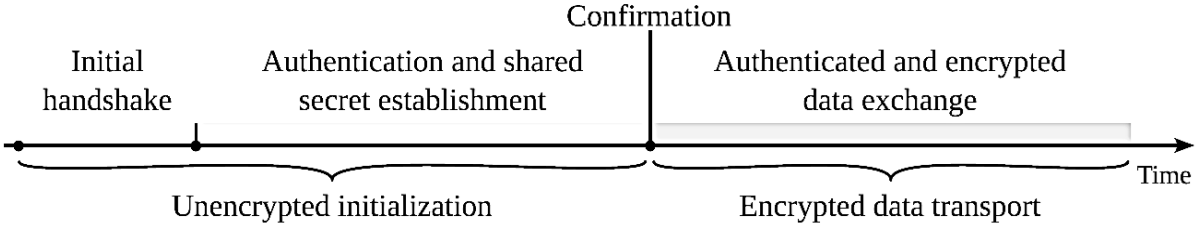

Figure 2.
Network Security Protocols [13]

***Development of in Network Security Technologies and their Evolution*:** The history of Virtual Private Networks (VPNs) goes back to the early days of the internet, especially during the 1990s, as the internet began expanding rapidly. Over time, VPN technology

has evolved in response to growing security concerns, the need for remote access, and the development of stronger encryption methods [14] Here's a look at how VPNs have developed: In the 1980s, businesses and organizations were starting to use computer networks for internal communication. As a result, there was a growing need for secure ways to connect remote employees or branch offices to central networks, especially through public communication lines, like telephone systems [15]. During this time, the concept of tunneling emerged. Tunneling involves wrapping private data in a protective "tunnel" so it can safely travel across untrusted networks (like the internet) without being intercepted or altered. This was the foundation of what would later become VPN technology **[16].**

PPTP (Point-to-Point Tunneling Protocol): In the early 1990s, **Microsoft** introduced **PPTP**, a protocol designed to allow secure connections over the internet for remote access to private networks. The key idea was to make data transmissions secure as they traveled across the public internet. PPTP was easy to use and integrated well with Microsoft's Windows systems, leading to its widespread adoption. However, it wasn't long before it became clear that PPTP had significant security flaws, particularly with weak encryption. As a result, it couldn't offer the level of protection needed for sensitive data [17, 18].

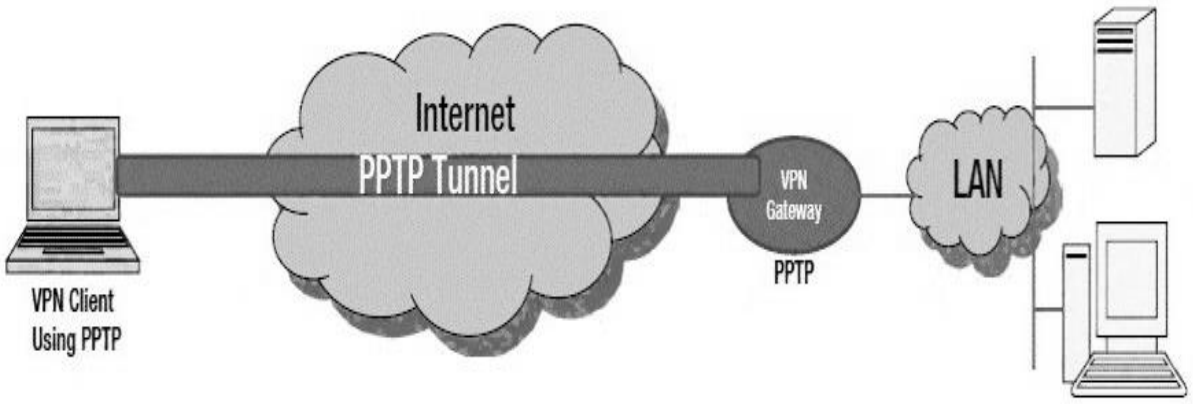

Figure 3.
PPTP based Network Security Protocols [13]

L2TP and IPsec: To address the shortcomings of PPTP, the Layer 2 Tunneling Protocol (L2TP)**.** While L2TP itself didn't provide encryption, it could be paired with another security protocol called **IPsec**. Together, they offered strong encryption and authentication, making L2TP/IPsec a much more secure solution for data protection.

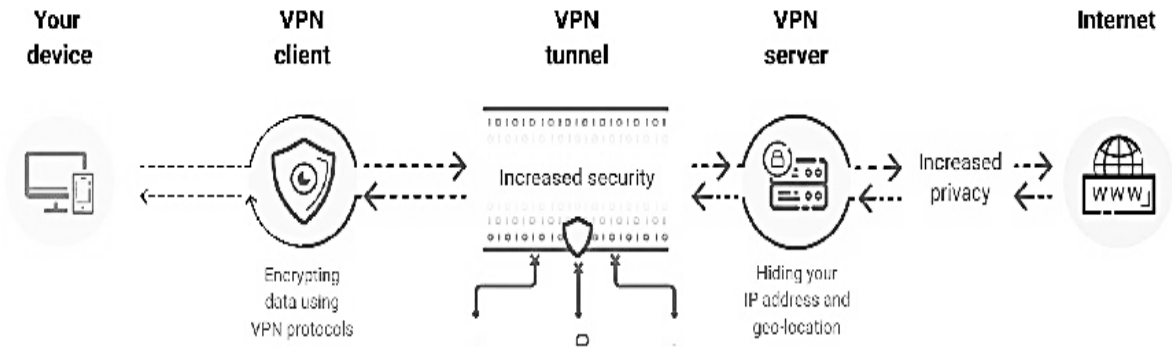

Figure 4.
L2TP based Network Security Protocols [14]

SSL VPNs emerged as a way to provide secure access to private networks using only a web browser. SSL, the same encryption protocol used for secure web browsing (like HTTPS), was adapted for VPNs to offer a simple, browser-based connection. The key advantage of SSL VPNs was their ease of use. They didn't require users to install special software, which made them highly accessible, especially for remote workers using various devices. SSL VPNs also allowed organizations to give access to specific web applications, rather than giving access to the entire network [15, 16].

OpenVPN was created as an open-source VPN protocol. OpenVPN stood out for its flexibility, robust encryption, and strong security. It could be configured to work on a wide variety of operating systems and devices, and it supported both SSL and IPsec encryption [17]. Thanks to its open-source nature, OpenVPN gained popularity for its transparency and reliability, and it became a widely adopted solution for secure, encrypted connections, even in complex network environments.

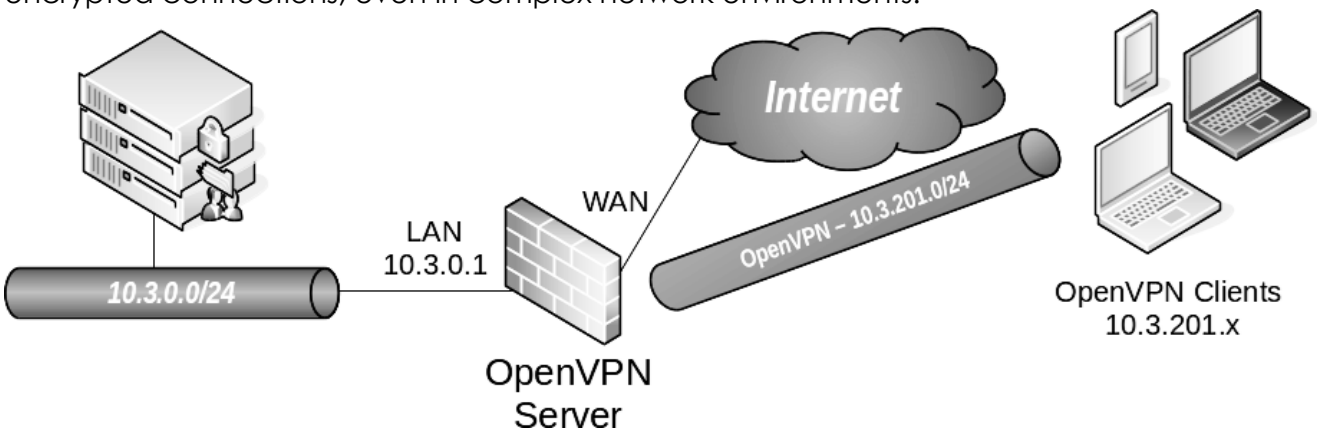

Figure 4.
OVPN based Network Security protocols [18]

IKEv2 (Internet Key Exchange version 2) emerged as a more modern and secure protocol, evolving from IPsec. Developed in the late 2000s, IKEv2 was particularly well-suited for mobile devices because it was fast at reconnecting and stable when switching between networks (for example, moving from Wi-Fi to mobile data). As smartphones and tablets became more popular, the demand for reliable VPNs that

could work seamlessly on these devices grew. IKEv2 quickly became a preferred option for providing secure connections on mobile networks [19, 20].
WireGuard was designed to be simpler, faster, and more secure than older protocols. Unlike its predecessors, WireGuard features a minimalistic codebase, making it easier to implement and audit for security flaws. WireGuard quickly gained attention due to its excellent performance and simplicity, making it a popular choice for both developers and users. It became a strong contender against established VPN protocols like OpenVPN and IKEv2, offering both speed and high-level encryption [21]. to protect privacy, ensure secure remote access, and safeguard sensitive information over the internet. With rising concerns over data privacy and the growing trend of remote work, VPNs have become more important than ever [22]. In addition, as more businesses embrace cloud computing, VPN technology has adapted to meet the needs of hybrid and multi-cloud environments. VPNs are now integrated with other security solutions, such as **Zero Trust** models [24, 25] and are being used alongside **software-defined perimeters** to create highly secure, flexible networks. In summary, VPNs have come a long way since their early days, continuously evolving to meet the demands of modern internet use. They have shifted from simple remote access tools to essential security technologies, helping protect users and organizations from a growing array of cyber threats [23].

LITERATURE REVIEW

In today's digital world, Virtual Private Networks (VPNs) have become essential tools for protecting privacy, securing data, and managing networks effectively. Whether for personal use or business, VPNs play a crucial role in ensuring that sensitive information remains safe and communications stay secure. Here's a breakdown of how VPNs impact modern business, personal privacy, and enterprise network security [26] As technology continues to evolve, so too does VPN technology. Next-generation VPNs are being designed to address the increasing complexity of modern networks. These new VPNs will include features like advanced traffic analysis, machine learning for detecting threats, and deeper integration with cloud security solutions, further strengthening the protection of data and connections across the internet [27, 28]. In the business world, VPNs are vital for ensuring secure communication, protecting company data, and supporting remote work. Here's how VPNs contribute to business operations:

Remote Work and Secure Access

As remote work becomes more common, VPNs are a lifeline for businesses, allowing employees to securely access company networks from anywhere. VPNs create a safe connection over the internet, ensuring that remote workers can access crucial resources without compromising security. Whether employees are working from home or different locations, VPNs ensure they can access company databases and applications securely, even on public Wi-Fi networks [29].

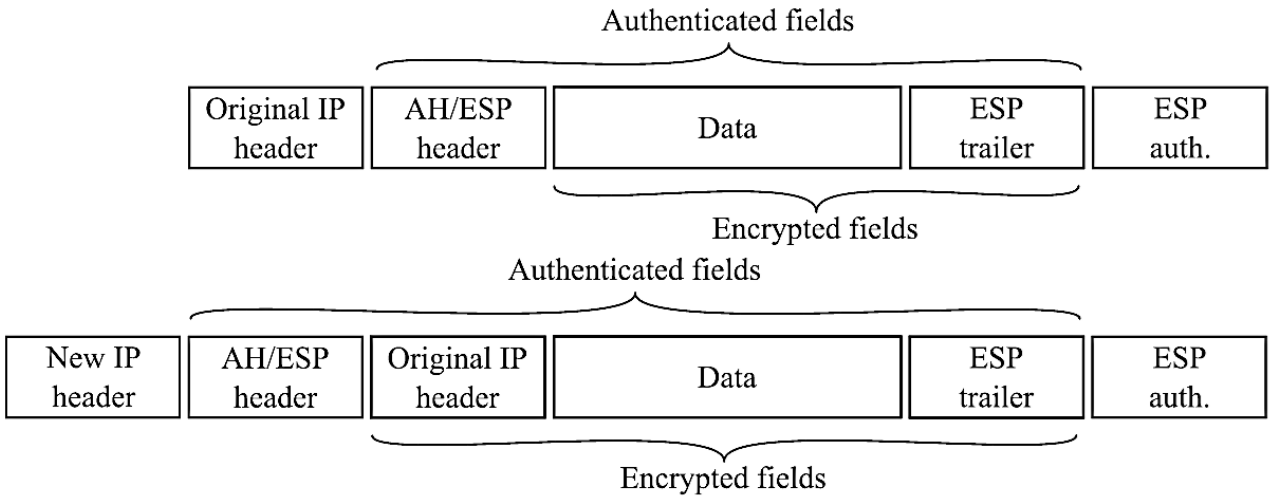

Figure 5.
Network Security Protocols (a) Transport mode (b) Tunnel mode [30]

Secure Communication Between Offices

For businesses with multiple offices or international branches, VPNs allow secure connections between them. This ensures sensitive data, like financial transactions or customer details, are safely shared over the internet, avoiding the risks of public networks [31].

Protection Against Cyber Threats

VPNs help businesses guard against cyber threats like hacking, phishing, and data interception. By encrypting data sent over the network, VPNs ensure that information remains secure and inaccessible to unauthorized users, which is especially important when dealing with sensitive customer data. VPNs allow businesses to set up secure, private networks using public internet infrastructure. This is a cost-effective alternative to setting up private networks, providing the same level of security for a fraction of the cost [32].

VPNs and Personal Privacy

For individuals, VPNs are increasingly important for maintaining privacy online and protecting personal data. Here's how VPNs help:

Anonymity and Masking Identity VPNs help users keep their identity private by hiding their IP address and routing internet traffic through a remote server. This makes it harder for websites, advertisers, and even governments to track online activities, providing greater anonymity. When using public networks, where data is vulnerable to interception, VPNs help protect users by masking their true location and keeping their browsing private [33]. VPNs are also useful for accessing content that's restricted by region. For instance, if a website or streaming service is unavailable in a user's country, a VPN can make it appear as though they're browsing from a different location, unlocking content. In countries with strict internet censorship, VPNs provide a way to access blocked websites and information without revealing the user's identity [34]. Public Wi-Fi networks, like those in cafes or airports, are often insecure and a target for hackers. VPNs provide an extra layer of security, protecting sensitive data like passwords and credit card information when users are on these networks.

Preventing Tracking and Surveillance

VPNs help prevent websites, internet providers, and even governments from tracking users' online activity. By encrypting data and hiding browsing patterns, VPNs allow users to browse freely without being constantly surveilled. For large organizations, VPNs are essential for securing networks, protecting business data, and supporting a global workforce. Here's how VPNs enhance enterprise security. Data Encryption using VPNs can encrypt all data sent across a company's network, making it unreadable to anyone trying to intercept it [35]. This encryption ensures that sensitive business data, like customer information and intellectual property, remains protected during transmission.

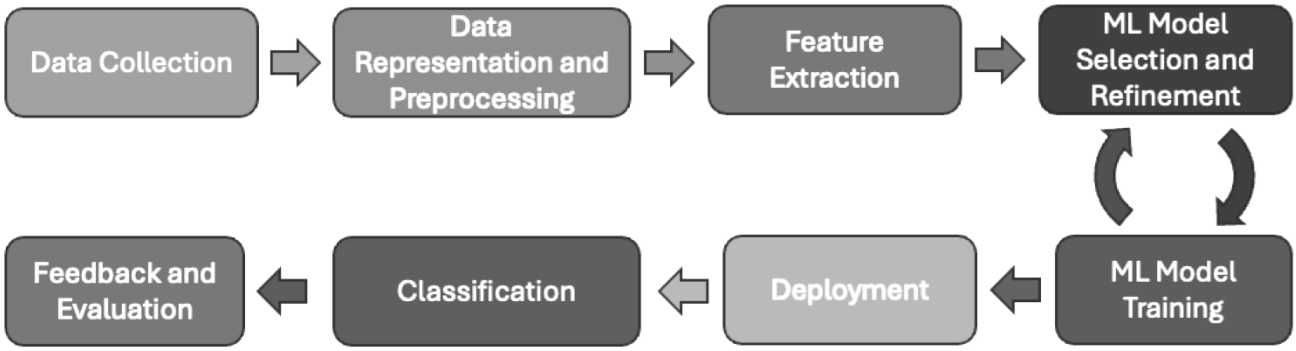

Figure 6.
ML based Encrypted network traffic analysis [36]

Many businesses operate across multiple regions with teams working from different locations. VPNs facilitate secure communication between these teams, ensuring that data can be shared and collaboration can happen without compromising security. VPNs also support secure video conferencing and voice calls, essential for remote teams and international business operations.

Network Segmentation and Access Control

VPNs allow businesses to create secure "zones" within their networks, limiting access to sensitive information based on employee roles. This means only authorized users can access specific data, preventing unauthorized access and enhancing security. For businesses in regulated industries, such as healthcare or finance, VPNs help ensure compliance with laws like GDPR or HIPAA. These regulations require companies to protect sensitive data, and VPNs are an important part of meeting these security standards. VPNs often include advanced features like threat detection, malware blocking, and intrusion prevention. These capabilities, along with other security tools like firewalls and antivirus software, help protect businesses from cyberattacks and data breaches [37].

Table 2.

Security Protocols Finding [38]

Focus area	Application	Main idea	Findings	Limitation
Deployment	Data center security	Security Risk analysis	Segregation of internal/ External nets via VPN	Overlooked testbed based performance limitations
Deployment	Use of VPNs in electric systems	Analysis	Use of VPN for reliable Urban Comm	Overlooked resource constraint environments
Deployment	Industrial Control Environment	Probabilistic Model for VPN Configs	Password complexity increases security	Only password strength & user count considered
Deployment	SCADA Systems	Analysis of CIA	Provided suggestions for future VPNs	Broader perspective, lacks in-depth analysis
Deployment	Enterprises	Study of SSL VPNs in network security	Phased approach of VPN Deployment	Comparison of results is overlooked
Deployment	Enterprises	Detailed overview of security controls and layer 3 VPNs	Studies VPN features against the NIST Controls	Other three important layers of security were not brought in comparison

In today's interconnected world, network security and privacy are more crucial than ever. As we rely more on digital platforms for both personal and business activities, the threats to our online security have grown significantly. Rapid technological advancements have brought greater convenience, but they've also introduced new vulnerabilities in how we communicate and share data. One of the most important tools to counter these threats is the Virtual Private Network (VPN), which helps ensure secure and private communication, especially over potentially unsafe networks like the public internet. However, cyber threats are constantly evolving. Sophisticated hacking techniques, data interception, and identity theft create significant challenges for network security. Additionally, the increasing rise of surveillance by governments, data collection by corporations, and even censorship complicate the ability to maintain personal privacy online. The research problem centers on understanding and addressing these growing challenges to network security and privacy. It's essential to explore why robust VPN protocols are necessary—protocols that not only ensure secure communication but also protect against emerging threats while maintaining privacy in the increasingly complex online world.

This research adopts a qualitative approach, focusing on the conceptual analysis of VPN protocols through an extensive review of existing literature. The goal is to gain insights into the operational mechanics, security features, and performance aspects of various VPN protocols. By leveraging academic papers, industry reports, and technical documentation, this approach aims to build a well-rounded understanding of how different VPN protocols function in modern network environments.

Data Collection

Several data collection methods will be employed to gather practical, real-world insights on VPN protocols: The research will include case studies from various sectors like healthcare, and enterprise, as well as from individuals who use VPN services. These case studies will explore the adoption, challenges, and benefits of different VPN protocols in real-world settings, offering a comprehensive look at their practical effectiveness and limitations.

Data on VPN performance will be gathered from service providers and network administrators to understand how different VPN protocols perform in everyday use. This includes metrics like encryption overhead, throughput, latency, and resource consumption during VPN use [39].

Surveys or interviews with network security professionals will provide additional insights into the practical challenges and preferences of implementing and managing VPN solutions. These discussions will help uncover common obstacles in deploying VPN protocols and how network administrators balance the need for security with performance considerations.

TESTING AND EVALUATION

The study will rigorously evaluate VPN protocols through the following methods. The research will compare different VPN protocols using key performance indicators:

- **Encryption Overhead:** Assessing how encryption impacts network performance, particularly how much it delays or affects data transfer speeds.
- **Latency:** Measuring the delay in data transmission when using various VPN protocols. This is especially important for time-sensitive applications like video streaming or VoIP calls.
- **Throughput:** Analyzing the volume of data that can be transmitted through the VPN connection per unit of time, reflecting the efficiency of each protocol.
- **Resource Usage:** Evaluating how much CPU and memory each VPN protocol consumes, especially on resource-constrained devices like smartphones and embedded systems.
- **Penetration Testing:** Using tools to simulate real-world cyberattacks on VPN implementations to identify vulnerabilities, such as weaknesses in encryption or susceptibility to man-in-the-middle attacks.
- **Vulnerability Assessments:** Automated security tools like OpenVAS will be used to conduct vulnerability scans on VPN systems to detect known flaws and ensure that the protocols are secure against contemporary cyber threats [40].

Case Study Analysis Across Different Sectors:

The research will also include an analysis of VPN implementations within specific business sectors to understand the particular challenges and benefits each protocol offers:

- **Healthcare Sector:** Exploring how VPNs are used to secure patient data and ensure compliance with healthcare regulations such as HIPAA.
- **Enterprise Sector:** Investigating how large corporations use VPNs to secure remote access and internal communications between offices [41].

1.1. Threats, Privacy and Challenges Concerns to Network Security:

- **Cyberattacks:** Threats like hacking, phishing, man-in-the-middle attacks, and malware seek to steal sensitive data or compromise the integrity of networks.
- **Data Interception:** Public networks, such as the internet, leave data vulnerable to interception, especially if it's not encrypted.
- **Insider Threats:** Even trusted individuals within organizations can intentionally or unintentionally leak sensitive information.
- **Government Surveillance:** Worries about mass surveillance and the unwarranted collection of personal data by governments and corporations have raised alarm about personal privacy.
- **Corporate Data Mining:** Many companies collect data for commercial purposes, leading to concerns about the misuse of personal information.
- **Loss of Anonymity:** Tracking and profiling by websites and service providers have led to the erosion of online anonymity.
- **Weak Protocols:** Some older VPN protocols lack the necessary security measures, leaving users exposed to attacks.
- **Performance Overhead:** Strong encryption often slows down internet speeds, which can be a deterrent, especially in high-traffic environments.
- **Compatibility Issues:** With various operating systems, devices, and network configurations, ensuring consistent VPN performance can be challenging.

The Need for Robust VPN Protocols:

- **Encryption and Authentication:** It's essential to develop VPN protocols that offer strong encryption to protect data during transmission and robust authentication methods to verify users and devices.
- **Flexibility and Scalability:** VPN protocols should be adaptable to different network architectures, allowing businesses and individuals to scale their security measures as needed.
- **Protection Against Emerging Threats:** VPN technologies must evolve to defend against new threats like quantum computing, which could potentially break existing encryption methods.

This research will delve into the development and evaluation of robust VPN protocols that address the challenges outlined above. Specifically, it will focus on:

- How the evolving nature of cyber threats impacts network security. The role of advanced encryption techniques and modern tunneling protocols in improving VPN security.
- The effectiveness of current VPN protocols in safeguarding data and privacy against emerging threats. The potential of next-generation VPN solutions, like WireGuard, which promise faster, more secure and more reliable connections. Balancing strong security measures with maintaining high performance and user convenience.

The main goal of this study is to provide a clear and in-depth look at Virtual Private Network (VPN) security protocols and how they help protect data and ensure secure communication. The focus will be on understanding the different types of VPN protocols available, analyzing their strengths and weaknesses, and determining which ones are best suited for various security needs. Key objectives of this study include:

- **Exploring VPN Protocols**: Looking into the basics of VPN protocols, such as OpenVPN, IKEv2/IPsec, L2TP/IPsec, PPTP, and newer options like WireGuard.
- **Understanding Encryption Methods**: Investigating how different VPN protocols use encryption and how it strengthens data security.
- **Authentication Techniques**: Examining the authentication processes within VPNs, including multi-factor authentication and certificates, to ensure only authorized users access the network.
- **Evaluating Protection Against Cyber Threats**: Assessing how well each protocol defends against common online threats like data interception, man-in-the-middle attacks, and eavesdropping.
- **Balancing Performance and Speed**: Analyzing how security and performance are balanced, helping to identify which protocols are most suitable for activities like streaming, gaming, or remote work.
- **Compatibility Across Devices and Networks**: Studying how VPN protocols work across different platforms and devices to ensure smooth operation in various settings.
- **Bypassing Censorship and Restrictions**: Investigating how certain VPN protocols can bypass geographical restrictions or government censorship, supporting internet freedom.

By tackling these challenges and exploring the importance of robust VPN protocols, this research aims to provide valuable insights into how VPN technologies can be improved. The goal is to ensure secure, private, and efficient communication as the cyber landscape continues to evolve. In today's digital world, where so much of our personal and professional lives happen online, keeping our data and communications secure is more important than ever. As cyber threats continue to grow more sophisticated, understanding different VPN (Virtual Private Network) security protocols becomes crucial for ensuring our information stays safe. VPNs are widely used to secure online activity, allowing us to communicate privately over potentially unsafe networks, such as the public internet. But not all VPN protocols offer the same level of protection, and picking the right one is essential for maintaining privacy and security. VPN protocols are what make it possible to securely transmit data over the internet. They establish a secure connection between a user's device and the remote server by using a combination of encryption and tunneling methods. The protocol you choose determines how strong the security is, how fast your connection will be, and how easily it can bypass things like firewalls or content restrictions.

Encryption Strength

Encryption is the foundation of any VPN because it makes sure that anyone trying to intercept the data can't read it. Some VPN protocols use stronger encryption than others, making them better at protecting sensitive information. For example, protocols like OpenVPN and IKEv2/IPsec use powerful encryption (AES-256), keeping your data secure. Older protocols like PPTP, on the other hand, offer weak encryption and should be avoided if you're trying to keep your communications private [41].

Authentication Mechanisms

Authentication makes sure that only authorized users can connect to a VPN. Some VPN protocols offer stronger authentication methods to prevent unauthorized access and attacks like man-in-the-middle (MITM). OpenVPN and IKEv2/IPsec, for instance, provide multi-factor authentication, requiring users to verify their identity through something like a password or certificate—adding an extra layer of security. Different VPN protocols are designed to protect against different types of cyber threats. Protocols like L2TP/IPsec and OpenVPN are good at stopping attacks like eavesdropping, data interception, and MITM attacks by combining solid encryption with secure tunneling. On the flip side, older protocols like PPTP are more vulnerable to these types of attacks because they don't provide strong encryption [42]. While encryption is essential for security, it can sometimes slow down your internet connection. Some VPN protocols, like OpenVPN, strike a balance between security and performance, but others, like IKEv2, are designed for speed. This makes IKEv2 ideal for mobile users who need fast and stable connections. It's important to consider the trade-off between security and speed when choosing a VPN protocol, especially if you need to do things like video calls or large file transfers [43].

VPN protocols vary in how well they work across different devices and operating systems. IKEv2, for instance, is great for mobile devices because it can reconnect quickly after a connection drop. OpenVPN is highly flexible and can work on nearly any platform, but it may require installing extra software. Picking the right protocol ensures your VPN will work smoothly across all your devices, whether you're on a desktop, smartphone, or connecting remotely [44].

Bypassing Restrictions

Many people use VPNs to get around geographic restrictions or censorship. Some protocols, like OpenVPN and IKEv2, are more effective at bypassing firewalls and content filtering systems, making them ideal for use in countries with strict internet censorship. Knowing how different VPN protocols work allows you to choose the best one for securely accessing restricted content. With the rise of cyber threats, data breaches, and widespread surveillance, using a reliable VPN protocol is no longer optional—it's essential. The right VPN ensures that your sensitive data is protected, your communications are secure, and your privacy is maintained, even in an increasingly hostile digital environment [45].

As the world of cyber threats continues to evolve, it's important for both individuals and organizations to understand the strengths and weaknesses of different VPN protocols. This knowledge helps you make informed decisions about which protocol is best suited to your needs, whether that's securing business communications, protecting personal privacy, or ensuring sensitive data stays private.In conclusion, understanding VPN security protocols is essential for anyone who values protecting their data and communications. As cyber threats grow more complex, choosing a VPN protocol with strong encryption, reliable authentication, and solid performance is key to ensuring that your online activities remain safe and private [46, 47]. Virtual Private Network (VPN) protocols are fundamental for securing internet communication. These protocols establish secure "tunnels" between a user's device

and the destination network, ensuring that sensitive data is safely transmitted over unsecured networks like the public internet. Below are some key VPN protocols:

- **PPTP (Point-to-Point Tunneling Protocol):** One of the earliest VPN protocols, PPTP offers fast speeds but is widely considered insecure today due to its weak encryption. As a result, it has been largely replaced by more secure alternatives.
- **L2TP (Layer 2 Tunneling Protocol):** L2TP itself does not provide encryption, so it is commonly paired with IPsec (Internet Protocol Security) for added security. While it is more secure than PPTP, it is still vulnerable to certain attacks if not configured correctly.
- **IPsec (Internet Protocol Security):** Often paired with other protocols like L2TP or IKEv2, IPsec is renowned for its robust encryption and authentication, ensuring data integrity and confidentiality.
- **OpenVPN:** OpenVPN is an open-source protocol that offers great flexibility and strong encryption. It utilizes SSL/TLS for key exchange, making it one of the most secure VPN protocols in use today.
- **SSL/TLS VPN:** These protocols use Secure Socket Layer (SSL) or Transport Layer Security (TLS) to encrypt communication. SSL/TLS VPNs are commonly used for web-based VPNs, especially for secure browsing and remote access.
- **IKEv2 (Internet Key Exchange version 2):** Known for its speed and security, IKEv2 is often paired with IPsec for encrypted communication. It is especially popular for mobile networks because of its ability to reconnect seamlessly after network disruptions.
- **WireGuard:** A newer VPN protocol, WireGuard has quickly gained popularity due to its simplicity, speed, and modern cryptography. While it is still relatively new, it is considered an efficient and secure alternative to older protocols like OpenVPN and IKEv2.

  VPN technology has undergone significant evolution since the 1990s when protocols like PPTP and L2TP/IPsec were initially introduced. Over time, as cyber threats became more sophisticated, these protocols evolved, incorporating stronger encryption, better performance, and enhanced security features. The move towards open-source protocols like OpenVPN and WireGuard reflects a growing focus on transparency, performance, and robust security.

Security Features

Encryption is central to VPN security. Modern protocols like OpenVPN and IKEv2/IPsec use robust encryption algorithms such as AES (Advanced Encryption Standard) with 256-bit keys, RSA for key exchange, and Diffie-Hellman for secure key establishment. These cryptographic methods ensure that transmitted data is protected from unauthorized access, even if intercepted. Authentication ensures that only authorized users can access the network [48]. Common methods include username/password combinations, certificates, and multi-factor authentication (MFA). Strong authentications mechanisms help mitigate the risks associated with man-in-the-middle attacks and credential theft. To prevent tampering, VPNs utilize mechanisms such as HMAC (Hash-based Message Authentication Code), ensuring the received data matches the sent data, verifying its integrity.

Tunnel Modes

VPNs typically operate in two modes Transport Mode and Tunnel Mode. In Transport Mode, only the data payload is encrypted, while the header (source and destination addresses) remains intact, making it more efficient for end-to-end communications. In Tunnel Mode, both the header and the payload are encrypted, providing additional security—this mode is often used for site-to-site VPNs [49]. OpenVPN and IKEv2/IPsec are considered some of the most secure VPN protocols, known for their robust encryption, frequent updates, and resistance to attacks. In contrast, PPTP is highly insecure and should be avoided, as it is vulnerable to brute-force and cryptographic attacks. WireGuard, though relatively new, offers strong security with modern cryptography but lacks the widespread support and extensive audit history of more established protocols.

Suitability for Different Network Environments:

Open VPN and IKEv2/IPsec are well-suited for enterprises requiring high security and compatibility across diverse devices. L2TP/IPsec may still be useful for legacy systems, but PPTP is not recommended due to its vulnerability for personal use, Wire Guard provides a good balance between speed and security, making it ideal for consumers who prioritize performance without compromising privacy. Open VPN is also a strong choice for users focused on security. In cloud environments, SSL/TLS VPNs are commonly used for secure web-based remote access. Open VPN and IKEv2/IPsec are also effective for securing cloud-to-cloud communications and remote connections [50].

Performance Metrics

Performance factors like speed, latency, and resource consumption are essential when evaluating VPN protocols. Wire Guard stands out for its high speed and low overhead, making it an excellent choice for performance-sensitive environments. Open VPN, while providing strong security, can suffer from slower speeds due to its complex encryption. IKEv2/IPsec offers a good balance between speed and security, particularly on mobile devices.

- **Secure Remote Access:** VPNs are widely used to provide secure remote access to corporate networks, allowing employees to connect to internal resources while maintaining security, even on public networks. OpenVPN and IKEv2/IPsec are often the protocols of choice for such scenarios.
- **Site-to-Site Connections:** VPNs are also used to create secure connections between different networks. Tunnel Mode and protocols like IPsec are commonly employed to ensure secure communication between remote offices or data centers.
- **Secure Browsing:** VPNs are popular for individual use, ensuring privacy and secure browsing, especially on public Wi-Fi. OpenVPN and WireGuard are commonly utilized due to their strong security features and user-friendly interfaces.

- **Corporate Networks:** Businesses rely on VPNs to safeguard sensitive data, secure internal communications, and protect privacy within their networks. Protocols like IKEv2/IPsec and OpenVPN are often deployed to ensure both confidentiality and integrity.
- **Emerging Trends:** As cloud computing and hybrid network models become more prevalent, VPNs are playing a critical role in securing communications between on-premise infrastructure and cloud-based resources. VPN-as-a-Service (VPNaaS) platforms are also emerging as scalable and secure solutions tailored to cloud environments.

Deep Dive into Security Features

VPN protocols integrate several advanced security features to safeguard data during transmission. These mechanisms are crucial in ensuring confidentiality, integrity, and authentication in any network environment: Advanced Encryption Standard (AES) is widely implemented in modern VPN protocols such as OpenVPN and IKEv2/IPsec. AES uses key lengths of 128, 192, or 256 bits, providing strong protection against potential decryption attempts. Its robust encryption ensures that intercepted data remains secure from unauthorized access. RSA encryption is a key component in securely exchanging keys between clients and servers. It relies on asymmetric encryption, where two keys (public and private) are used for encrypting and decrypting messages, ensuring that data remains protected during the key exchange process. Mechanisms like HMAC (Hash-based Message Authentication Code) validate the integrity of data, ensuring that transmitted information has not been tampered with. This is essential in preventing man-in-the-middle attacks, where attackers could alter the data without detection.

Modern Network Environments:

- **The Role of VPNs in Cloud-Based Environments:** VPNs are essential in securing communication between on-premises infrastructure and cloud resources. With the rise of hybrid and multi-cloud environments, VPNs ensure that data exchanged between on-premise systems and cloud services remains private and protected.
- **Integration of VPN Protocols in Hybrid IT Infrastructures:** Hybrid infrastructures, which combine on-premises and cloud services, require secure communication between systems. Protocols like IKEv2/IPsec and OpenVPN are ideal for securing these connections, allowing organizations to scale and remain flexible as their infrastructure grows.
- **VPN Challenges in the Era of Mobile Devices, Remote Work, and IoT:** With mobile devices, remote work, and IoT becoming central to modern networks, VPNs must adapt to meet these new demands. VPN protocols must ensure reliable, secure access for a wide variety of devices. Challenges include securing mobile endpoints, preventing unauthorized access, and supporting the massive scale required by IoT devices.

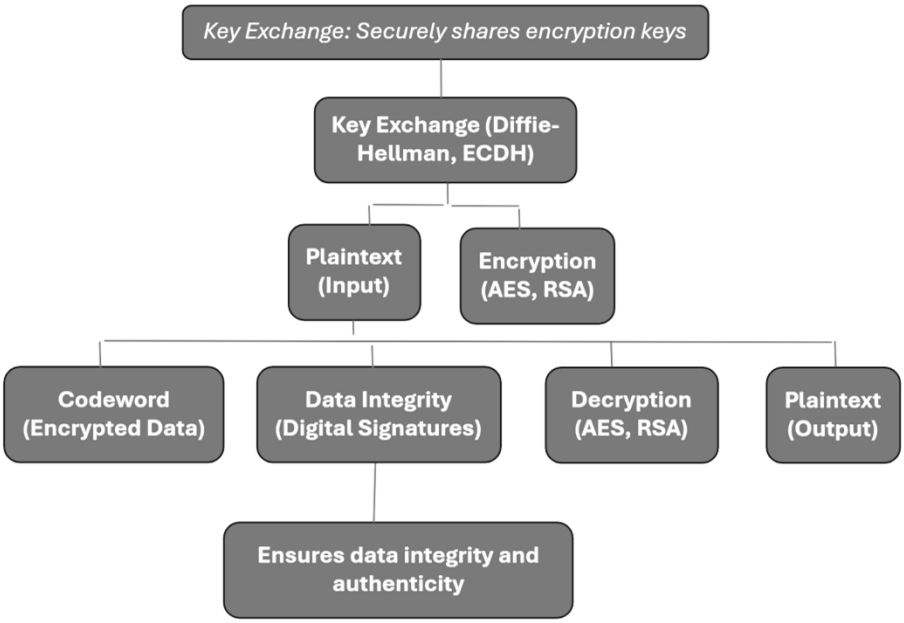

Figure 5: Plain text to Codeword Conversion using Cryptographic Algorithms for Data Traffic Security [51].

VPN traffic security protocols are integral to securing networks today, but their ability to evolve alongside emerging technologies and threats is crucial. By understanding the strengths, weaknesses, and specific use cases of each protocol, organizations can select the best VPN solution to meet their needs while ensuring robust security, privacy, and performance.

CONCLUSION AND RECOMMENDATIONS

In this paper, we presented an overview of current approaches for the classification and analysis of encrypted traffic specialy virtual private network. First, we selected a number of the most widely used encryption protocols and described their packet structure and standard behaviour in a network. Second, we focused on information that is provided by encryption protocols themselves. VPN protocols are crucial for securing modern networks, but choosing the right one depends on the specific needs and conditions of each environment. Organizations must weigh factors like security requirements, performance needs, network size, and workforce demands when selecting a VPN solution. As technology continues to evolve, ongoing research and development will be necessary to keep up with emerging challenges, including the rise of quantum computing and the increasing complexity of network infrastructures.

Summary of Findings:

The analysis of various VPN security protocols highlights that each one has distinct advantages, drawbacks, and suitable use cases depending on the network environment. Below is a recap of the key findings:

- **PPTP:** While PPTP offers fast connections, its serious security vulnerabilities make it unsuitable for modern networks. Its weaknesses make it easy for attackers to decrypt communications, so it is no longer recommended for use.
- **L2TP/IPsec:** Combining L2TP with IPsec enhances security, but the protocol is still susceptible to misconfigurations. It's viable for legacy systems or environments that don't require the highest levels of security but should be used cautiously.
- **OpenVPN:** OpenVPN is widely respected for its strong security and flexibility, supporting various encryption algorithms. It can work well in a variety of network environments. However, the performance may be impacted due to its encryption overhead, particularly in devices with limited resources.
- **IKEv2/IPsec:** Known for its fast speeds, stability, and ability to handle interruptions, IKEv2/IPsec is ideal for mobile networks. Its robust encryption and authentication make it a top choice for many organizations, though configuring it may be more complex than other protocols.
- **WireGuard:** WireGuard's modern cryptographic design, simplicity, and efficiency make it a standout option. It delivers faster performance than older protocols, though it's still new and lacks the extensive security audits of more established protocols. Its use may not be suitable in all environments, especially those requiring legacy support.

Recommendations:

- **For Organizations:** Organizations should carefully select a VPN protocol based on their unique security needs, performance requirements, and infrastructure. Here are some considerations for different environments:
    - **Enterprise Networks:** For large-scale, high-security environments, **OpenVPN** and **IKEv2/IPsec** provide robust encryption and flexibility. To further secure access, multi-factor authentication (MFA) and strict access control policies should be implemented alongside these protocols.
    - **Mobile Networks:** For mobile networks or environments with frequent network changes, **IKEv2/IPsec** is an excellent choice due to its resilience against disruptions and strong security. It's particularly suited for businesses with remote or mobile workforces.
    - **Home and Small Networks:** For home users or small-scale networks, **WireGuard** offers an ideal mix of security and performance, with a simple setup and low overhead. It's perfect for those who need a fast and secure VPN without complex configuration.
    - **Cloud and Hybrid Environments:** For cloud-based or hybrid IT infrastructures, **SSL/TLS VPNs** and **IKEv2/IPsec** are effective in securing communications between on-premise and cloud systems. These protocols ensure encryption, integrity, and authentication in dynamic environments where scalability and flexibility are essential.
- **For Future Research:** There are several promising avenues for advancing VPN technology:
    - **AI in VPN Security:** As cyber threats grow more sophisticated, AI could play a critical role in enhancing VPN security. AI could dynamically adjust VPN settings in real-time, detect security anomalies, and proactively mitigate threats.

- **Post-Quantum VPN Protocols:** As quantum computing advances, many current encryption techniques could be vulnerable. Research into quantum-resistant algorithms and the development of VPN protocols that can withstand quantum threats will be vital to maintaining data security in a post-quantum world.
- **VPN Optimization for IoT:** The rapid growth of IoT devices presents new challenges for VPNs. Future research should focus on optimizing VPN protocols for devices with limited resources, ensuring secure and seamless connections across large, distributed IoT networks..

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the supervisors and their different affiliations.

Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.

Availability of data and material: In the approach, the data sources for the variables are stated.

Authors' contributions: Each author participated equally to the creation of this work.

Conflicts of Interests: The author declares that there is no conflict of interest related to this study. All research activities, data collection, and analysis were conducted with full transparency and impartiality. No financial or personal relationships that could influence the research outcomes exist. The findings and conclusions presented in this work are solely based on the data collected and the academic analysis carried out throughout the study.

Consent to Participate: Yes

Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

1. Tahir, R. A study on malware and malware detection techniques. Int. J. Educ. Manag. Eng. , vol. 8, no. 20, 2018.
2. Aliyyah Rosyidah1 , Jumadi Mabe Parenreng, "Network Security Analysis Based on Internet Protocol Security Using Virtual Private Network (VPN)" July, 06 2023
3. Leukfeldt, E.R.; Kleemans, E.R.; Stol, W.P. Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. Br. J. Criminol. 2017, 57, 704–722.
4. Alenezi, M.N.; Alabdulrazzaq, H.; Alshaher, A.A.; Alkharang, M.M. Evolution of malware threats and techniques: A review. Int. J. Commun. Netw. Inf. Secur. 2020, 12, 326–337.
5. Ghafir, I., Hammoudeh, M., Prenosil, V., Han, L., Hegarty, R., Rabie, K., & Aparicio-Navarro, F. J. (2018). Detection of advanced persistent threat using machine-learning correlation analysis. Future Generation Computer Systems, 89, 349-359.
6. Joloudari, J. H., Haderbadi, M., Mashmool, A., GhasemiGol, M., Band, S. S., & Mosavi, A. (2020). Early detection of the advanced persistent threat attack using performance

analysis of deep learning. IEEE Access, 8, 186125-186137.
7. Reddy, B. I., & Srikanth, V. (2019). Review on wireless security protocols (WEP, WPA, WPA2 & WPA3). International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 5(4), 28-35.
8. Halbouni, A., Ong, L. Y., & Leow, M. C. (2023). Wireless Security Protocols WPA3: A Systematic Literature Review. IEEE Access.
9. Ambavkar, P. S., Patil, P. U., Meshram, B. B., & Swamy, P. K. (2012). Wpa exploitation in the world of wireless network. Int J Adv Res Comput Eng Technol, 1(4), 609-618.
10. Cahyadi, D., Astuti, I. F., & Nazaruddin, N. (2023, February). Comparison of throughput and CPU usage between WPA3 and WPA2 security methods on wireless networks 802.11 n. In AIP Conference Proceedings (Vol. 2482, No. 1). AIP Publishing.
11. Baray, E., & Ojha, N. K. (2021, April). WLAN security protocols and WPA3 security approach measurement through aircrack-ng technique. In 2021 5th International conference on computing methodologies and communication (ICCMC) (pp. 23-30). IEEE.
12. Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",sss Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019
13. H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023
14. Khan, S., Ullah, I., Khan, H., Rahman, F. U., Rahman, M. U., Saleem, M. A., ... & Ullah, A. (2024). Green synthesis of AgNPs from leaves extract of Saliva Sclarea, their characterization, antibacterial activity, and catalytic reduction ability. Zeitschrift für Physikalische Chemie, 238(5), 931-947.
15. S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024
16. H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018
17. Waleed, A. Ali, S. Tariq, G. Mustafa, H. Sarwar, S. Saif, I. Uddin, "An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications", Bulletin of Business and Economics (BBE)., vol. 13, no. 2, pp. 200-206, July. 2024
18. Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.
19. Noor, A. Ilyas, Z. Javaid, H. Khan, "Framing a Knowledge Domain Visualization on Green Human Resource Management: A Bibliometric Analysis from 2008-2022", Pakistan Journal of Humanities and Social Sciences., vol. 11, no. 4, pp. 4200-4212, Aug. 2023
20. M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019
21. Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing

sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

22. U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023
23. Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019
24. Ali, M., Khan, H., Rana, M. T. A., Ali, A., Baig, M. Z., Rehman, S. U., & Alsaawy, Y. (2024). A Machine Learning Approach to Reduce Latency in Edge Computing for IoT Devices. Engineering, Technology & Applied Science Research, 14(5), 16751-16756.
25. Khan, A. Yasmeen, S. Jan, U. Hashmi, "Enhanced Resource Leveling Indynamic Power Management Techniqueof Improvement In Performance For Multi-Core Processors" ,Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019
26. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Oct. 2018
27. Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (AI) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power IoT Devices in 5G Networks. Spectrum of engineering sciences, 2(3), 528-586.
28. H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018
29. Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.
30. Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023
31. Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.
32. Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019
33. Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020
34. Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019

35. Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018
36. Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.
37. Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019
38. Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020
39. Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023
40. Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018
41. Javed, M. A., Anjum, M., Ahmed, H. A., Ali, A., Shahzad, H. M., Khan, H., & Alshahrani, A. M. (2024). Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced Anomaly Detection in High-Dimensional Datasets. Engineering, Technology & Applied Science Research, 14(6), 17894-17899.
42. Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020
43. Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.
44. Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, "An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning", Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024
45. Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024
46. Naveed, A., Khan, H., Imtiaz, Z., Hassan, W., & Fareed, U. (2024). Application and Ethical Aspects of Machine Learning Techniques in Networking: A Review. Spectrum of engineering sciences, 2(3), 455-501.
47. Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023
48. Sebbar, A., Boulahya, S. E., Mezzour, G., & Boulmalf, M. (2016, May). An empirical study of wifi security and performance in morocco-wardriving in rabat. In 2016 International Conference on Electrical and Information Technologies (ICEIT) (pp. 362-367). IEEE.
49. Sagers, G., Hosack, B., Rowley, R. J., Twitchell, D., & Nagaraj, R. (2015, January). Where's the security in WiFi? An argument for industry awareness. In 2015 48th Hawaii

international conference on system sciences (pp. 5453-5461). IEEE.
50. Zhang, S., Venkatnarayan, R. H., & Shahzad, M. (2020, December). A wifi-based home security system. In 2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS) (pp. 129-137). IEEE.
51. Hooper, M., Tian, Y., Zhou, R., Cao, B., Lauf, A. P., Watkins, L., ... & Alexis, W. (2016, November). Securing commercial WiFi-based UAVs from common security attacks. In MILCOM 2016-2016 IEEE Military Communications Conference (pp. 1213-1218). IEEE.