Journal of Engineering, Management and Information Technology

ASPUR PUBLISHING

Vol. 05, No. 01 (2027) 17-28, doi:10.61552/JEMIT.2027.01.003 - http://jemit.aspur.rs

THE STUDY OF VIRTUAL PRIVATE NETWORKS (VPNS): AN ASSESSMENT OF SECURITY PROTOCOLS AND HOW THEY ARE USED IN TODAY'S NETWORKS

Israa Chyad [1]

Received 04.08.2026.
Revised 14.09.2026.
Accepted 28.10.2026.

Keywords:

VPN, Cybersecurity systems, Application, Networks.

Original research



A B S T R A C T

Virtual Private Network (VPN) is an essential piece of equipment for ensuring secure communications over public networks, and aids users secure their connection to a public network. This paper will explain the various security protocols that can be implemented and how these can be used on the current network architecture using a VPN. As VPNs play a crucial role in ensuring communication security on an insecure network, part one of the paper outlines a description of VPNs. Part two of the paper tells a little history about VPN technology, starting from the old days of IPSec, SSL/TLS and continuing to today's technology, such as Wireguard and QUIC. In part three, the various technologies and characteristics that make each type of technology safe, efficient and appropriate for each type of network is described. Last but not least, the authors provide practical, real-world examples of using VPNs in today's applications: Remote access, Site to site, Securing Data Being Sent Over Cloud Based Services. Therefore, VPNs play a critical function in developing a safe communication network in today's digital society.

© 2027 Journal of Engineering, Management and Information Technology

1. INTRODUCTION

One of the main elements of the network architecture of today is the Virtual Private Network (VPN). The Virtual Private Network (VPN) is not only an important part of today's network architectures, but is also crucial for companies to establish secure connections between their private networks and other public or unsecured networks (Bhagat, 2021). Organizations required to send data over a public network like the internet in a secure manner, and also to make sure the data being sent was complete, private and accessible. The main purpose of using a VPN is to create a secure tunnel between two points through encryption to ensure that no third party can listen, intercept or alter the sensitive data being transferred(Akinsanya et al., 2024). Historically, a VPN was mostly used to enable remote employees to gain access to corporate networks and similar resources ,With the technology it has undergone, however, the VPN has grown a great deal these days. VPN has been a part and parcel in the present business networking (Tymoshchuk et al., 2024) where a lot of service providers, geographically separated sites are available. With more and more companies going remote and relying on cloud-based solutions, VPN is a must-have for organizations to connect their networks securely, efficiently and on a scalable level. There are various security protocols that have been designed so as to allow for VPNs with different characteristics and security levels (Akinsanya et al., 2024; Ostroukh et al., 2024). Secure web-based communication is generally accomplished via SSL/TLS protocols, and offer secure access to online applications

[1] Corresponding author: Israa Chyad
Email: Asraaadnan74@mail.com

(Kosanam et al., 2024). However, in recent years there have been new protocols such as WireGuard and QUIC that have been found as potential alternatives to VPN protocols (Lafourcade et al., 2024). The newer protocols are designed to provide better performance, security and users experiences compared to the traditional VPN technologies. As the network advances, VPNs continue to play a crucial role in the cybersecurity infrastructure (Shim et al., 2025) because of the importance of transparent communication between users, devices and services. Therefore, the adoption of the VPN technology is a part of the organizations' cybersecurity measures aimed at network operations security and privacy (Mishko et al., 2024). Today, many activities rely on networks and the need to secure and ensure safe communication and information exchange with these networks is more important than ever; VPNs play a key role in this.

Configuration data is the most vital type of data needed to manage VPNs of all types. This information consists of protocol, encryption algorithm, authentication protocol and tunnels used for VPN. All these factors play a crucial role in creating a safe and effective VPN arrangement. They are also aware of how to set up and operate VPN in organizations. VPN deployments are usually assisted by these kinds of datasets to detect the possible security vulnerabilities and decide how to deploy the VPN, based on the organization security policies and strategies and cost minimization and efficiency maximization. Alia et al. (2024) recommended that the administrators should keep track of the data being transferred for every user session as well as analyse and review them. The network log details will include IP addresses, port numbers etc., which will provide detailed information on the activities in the VPN tunnels (sclient, dclient etc) and these logs will be valuable for detection purposes as security threats such as Malware infection, Data breach etc can be detected from these logs. There are other types of events that happen when using the VPN product, however, such as security log events, failed authentication attempt events, failed start-up attempts events and intrusion attempts events (Alia et al., 2024; Jevremovic et al., 2024). In either case, it is crucial to the safety, efficiency and compliance of the VPN system. At the present moment, the continuous monitoring is seen as a way to enhance security and enable organizations to constantly assess their security situation and act promptly to emerging threats (Patil & Korde, 2018). This can only be accomplished if there are wide trunked logs. The metrics are used by the organizations to see if its VPN works optimally or not and also for optimising the IP setting of its VPN for its best performance. Great attention is paid to dealing with the authentication data and thus, security is greatly enhanced and only the legitimate user can access the resources of the organization, and no illegally users are allowed. Lastly, compliance with regulations and industry standards like the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standard (PCI DSS) is crucial for the deployment and operation of VPN systems. Thus, to meet the compliance, the VPN systems should meet the legal requirements, industry requirements. T Furthermore, these datasets can be helpful for documenting security modification aspects, creating audit trails, and for forensic investigations, if needed. The above mentioned datasets are used by organisations for regulatory compliance, to ensure VPN security. Organizations have started to systematically acquire these datasets, analyse them and use them to enhance the security of their VPNs, as well as to identify the best VPN solutions currently available in the market for them to use to run a fast VPN to support their business operations (Forbacha & Agwu, 2023). Organisations can properly control the business implications of these datasets professionally and according to best practices of the industry, which ensures protection of the organisation's business network infrastructure.

There are plenty of studies available and can be located in the Virtual Private Networks (VPNs). However, there has been a lack of attention to some researchers (Hritcan et al., 2025; Manulal, 2024). So far, despite the huge amount of literature, there is not a wealth of information on the ‘security capabilities' of GPUs and whether or not they are suitable for specific applications. Similarly, no performance and comparative evaluations of the security protocols of VPNs (Mohamed & Kurnaz, 2024; Tian et al., 2024) have been conducted. Unlike IPSec and SSL/TLS, there has been a certain amount of focus of research done on WireGuard, however, there is no such detailed and comparative analysis of the three technologies and their effect on the use of the organizations in any realworld scenarios as that of Atadoga et al. (2024a) and Zela et al. (2024). Furthermore, scarce information about the support of implementing VPNs with the current network infrastructure and technology 5G and the Internet of Things (IoT) (Ajala et al., 2024; Tyshchenko et al., 2024). Hence, more research is needed on two things: how can VPN be used to build a secure network in 5G network and its components; and what are the challenges to be faced in implementing VPN in the 5G environment? Furthermore, a limited number of studies have been done to identify the correlation between the implementation of the VPNs and other security implementation frameworks such as Intrusion Detection and Prevention Systems (IDPS) and Security Information and Event Management (SIEM) Systems (Zela et al., 2024). Therefore, it is essential to have a grasp of the ways VPNs can be integrated into these security measures to enhance network security and protect against threats. This research gap will enable researchers to improve the security, performance and flexibility of VPNs to new technologies. This is a novel research and currently no research is done on this topic, but the integration of these technologies with VPN (Virtual Private Network) to strengthen the security of a network and increase threat detection capabilities can be investigated (Wang et al., 2024). Despite the vast amount of knowledge available in the literature, the research has provided valuable

recommendations for further development of VPN technology, security enhancements and applications. It will be important to complete this when doing research. In the modern highly interconnected network systems, the security and efficiency of VPNs can be enhanced using this approach, as described by Ogungbemi et al. (2024) and Tyshchenko et al. (2024).

2. LITERATURE REVIEW

VPN is considered as an essential element of modern network architectures because of its capabilities to enable secure communication over public networks" (Manulal, 2024). Topics covered in VPN literature range from the history and development of VPN technology, the authors development of security protocols and the use of VPN solutions in the current network environment (Ogundipe, Babatunde & Abaku, 2024). One of them is the history of VPN technology (Ogundipe, 2024, Sharma et al., 2024). The first application of VPN technology was to provide a secure connection between the remote workers and the corporate network to enable remote workers to access the corporate network from their remote offices . In fact, the function of VPNs has grown to greater than just site connections, and today VPNs are a vital means of protection for cloud servers from hackers and unauthorized users (Ramly et al., 2024; Zela et al., 2024). With increasing cybersecurity concerns and the increasing migration of workloads to the cloud, VPNs are playing an even more vital role in safeguarding data while in transit and ensuring that no one accesses the data without permission. As part of our literature review on VPNs, we look at the evolution of VPN technology and consider how VPN security protocols have been evolving and adopted (Filipescu et al., 2024; Jumakhan & Mirzaeinia., 2023). There are several different types of security protocols in use today that are capable of being used to secure communications over public networks, such as IPSec, SSL/TLS, WireGuard and QUIC. Due to the differences in performance and security of each protocol, it is still being debated by the researchers as to what the most suitable protocol would be for different scenarios (Sharma el al, 2024). Researchers have also been interested in VPNs as they help the security practitioners ensure the confidentiality, integrity and availability of information flowing through public networks (Ajala et al., 2024; Gentile et al., 2024). When using the internet via public networks, VPNs provide extra security and safeguard against unauthorized access and use through the use of strong security protocols and encryption methods.VPNs also feature comprehensive security protocols and encryption techniques to ensure their safe use and protect sensitive data from being accessed by unauthorized users when connected to public networks (Ayinla et al., 2024; Saad et al., 2024). Manulal (2024) and Forbacha and Agwu (2023) present some of the considerations and challenges of deployment and management of VPNs. The researchers identified four key factors that help in the successful implementation of a VPN: scalability, interoperability, regulatory factor and security factor. All four of these elements, however, are crucial to take into account when assessing the effectiveness of a VPN solution, and organisations must be diligent in evaluating their VPN solutions to ensure they are performing at their best and are secure. Implementing and deploying Virtual Private Networks (VPNs) for an organization comes with a number of challenges. Since the technology of the VPNs has improved, so has the security protocols as the organizations' requirements change with time from their networks (Kjorveziroski et al., 2024). This paper is aimed at providing information to the organizational decision makers regarding the possible deployment of VPN that can enhance network security and overall network performance (Fu et al., 2024; Sharma et al., 2024). The researchers point out that VPNs (Ajala et al. 2024, Gentile et al. 2024) can be used to enable organisations to send data confidentially without putting security at risk when using public networks. VPNs offer security that prevents possible breaches like eavesdropping, data tampering, and data interception (Ayinla et al., 2024; Saad et al., 2024). VPNs have been engineered to have high security and authentication protocols and encryption to prevent potential threats like eavesdropping, data interception, and manipulation (Ayinla et al., 2024; Saad et al., 2024). Therefore, VPNs are crucial for businesses seeking to improve the security of their networks and safeguard their data. Although VPN can provide many advantages, its deployment and management can pose a challenge for organizations (Forbacha & Agwu, 2023; Manulal , 2024). Scalability and interoperability, along with regulatory and possible vulnerabilities concerns arise for organizations. Thus, organizations that want to deploy VPN solutions need to be knowledgeable about their needs and have to choose VPN technologies that can provide them with network security and reliability at high levels and meet the requirements they have. This paper presents a comprehensive literature review of VPNs-related technologies, including an overview of the development of security protocols and implementation of VPNs in today's networks (Zela et al., 2024). The information assists the decision makers of the organization to make a definite decision as to the type of VPN deployment, the key findings and emerging trends in the technology of VPN (Fu et al., 2024; Sharma et al., 2024). Having these facts on board, organisations can be certain their VPN infrastructure will be suitable to their current requirements and future requirements for space on the network.

3. RESEARCH OVERVIEW

3.1. Problem Statement

VPN technologies are increasingly being used because they enable the protection of the communication infrastructure. But, many challenges and issues are still surfacing. One of the more common challenges/issues

being raised today is which security protocol to use to secure confidential, available, and integral data; how to use that protocol; and comparing the various security protocols being available today (including but not limited to IPsec, SSL/TLS, WireGuard, QUIC) to determine which is most appropriate for an organization, based on the security requirements, ease of use/performance characteristics, and compatibility with an organization's existing network infrastructure. The second major challenge in this modern world is the scalability. If there's a lot of network traffic or organisation is making use of VPNs on a larger scale, they might face scaling issues. Additionally, organisations must ensure that if their network expands they have the same amount of VPN capacity and that it performs at the same level and security prior to expansion. Finally, organisations need to integrate their newly deployed VPN into their existing network/security infrastructure without causing disruptions to their existing users. VPN technology is one of the security technologies which when used together with other security technologies like IDPS and SIEM would help an organization to have a better security posture. Organizations with sensitive data have a lot of regulation requirements that require them to implement a VPN that fulfills the regulatory compliance requirements outlined in the regulations (e.g., creating/implementing plans to ensure compliance with GDPR and HIPAA). The goal of this research is to discuss issues (in particular security protocols and the implementation of the security protocols) organizations may face when they deploy/manage VPN technology in today's modern networks. To address these challenges organisations can put in place practical solutions that will enhance the security of VPN technology, enable rapid deployment of VPN technology and boost security across the organisations network or data environment.

3.2. Objectives

The purpose of this paper is to provide an up-to-date overview of the VPN marketplace, and to review the types of security that VPN service providers provide. The purpose of this paper is also to evaluate the importance of these security features in today's network environment. There are other objectives that need to be covered in the rest of this document:

- Case study: Evolution of VPN technology and the importance of VPNs for the security of data when sending over an unprotected network.
- This study investigates different security mechanisms (protocols) that are used in VPNs, namely IPSec, SSL/TLS, WireGuard and QUIC, compares their security features, and compares their performance. The study also makes a comparison of the security mechanisms at the end to find the most suitable mechanism for different types of applications.
- The main purpose of this paper is to learn about the Virtual Private Network (VPN) technology in the present world of networks. We plan to explore this in particular, and how VPNs can be used to allow for remote users to connect to a corporate network; how VPNs can be used to link multiple geographically separated locations; and how VPNs can be used to provide secure access to cloud-based services.
- Some of the issues and problems with using VPNs in today's network environments and the requirements for implementing and maintaining VPNs may be (but are not limited to): The ever increasing demand for more capacity in the network, ensuring compatibility with all devices, and meeting regulatory requirements.
- This manual provides a general description of a virtual private network (VPN), and a couple of tips about how to ensure that your organization's VPN implementation is as effective as it can be.

The body of knowledge on VPNs needs to be available to anyone wanting to use them in order to enhance the security and performance of their networks.

3.3. Comparative Analysis of VPN Security Technologies

Virtual Private Network (VPN) technologies employ different security architectures and communication mechanisms to protect data transmitted across untrusted networks. However, their suitability for particular network environments depends on several factors, including their underlying technical architecture, cryptographic mechanisms, key management, network mobility, compatibility with network infrastructure, and performance characteristics. Therefore, evaluating VPN technologies requires a structured comparison rather than a general description of their security benefits.

This study compares four technologies: IPsec VPNs, TLS-based VPNs, WireGuard, and QUIC-based tunneling. These technologies differ in their design principles and intended functions. IPsec provides security at the IP layer, whereas TLS-based VPNs use Transport Layer Security to protect communications within VPN implementations. WireGuard is a VPN protocol designed around a relatively compact set of modern cryptographic mechanisms. In contrast, QUIC is a secure transport protocol that can serve as a foundation for tunneling applications but is not, by itself, a complete VPN protocol. Recognizing these distinctions is essential to ensuring a technically meaningful comparison.

Accordingly, the comparison considers the technical foundation, encryption and key management, Network Address Translation (NAT) and firewall traversal, network mobility, performance considerations, and typical deployment scenarios. Table 1 summarizes the principal characteristics of the four technologies and provides a framework for identifying their respective strengths, limitations, and potential areas of application. The comparison is intended to support technology selection according to specific operational requirements rather than to establish a universally superior solution.

Table 1. Benchmark for comparison of four technologies

Benchmark for comparison	IPsec VPN	TLS-based VPN	WireGuard	QUIC-based tunneling
Technical Layer or Foundation	IP-level security	Relies on TLS to secure the connection	VPN protocol that employs modern encryption	Secure transport over UDP, which can be used to establish tunnels
Cryptography and Key Management	Based on a set of protocols and configurations often IKEv2 for key management	Depends on the TLS version, authentication mechanism, and configuration	Specific cryptographic design and a key mechanism based on public keys	Relies on TLS 1.3 in the standard QUIC protocol
Bypassing NAT and firewalls	Possible, including NAT-T	Often suitable for environments that allow TLS over TCP or other supported transport methods	Uses UDP and may be affected by UDP blocking	Uses UDP and may be affected by UDP blocking or restriction
Network switching	Depends on the application and configuration	Depends on the implementation and the reconnection mechanism	Supports changing the endpoint address while maintaining the connection, provided that the necessary conditions are met	Supports connection migration, subject to protocol requirements and implementation details
Performance	Affected by implementation, encryption, and hardware	Affected by the transport mode and implementation Relatively simple design, but actual performance	requires measurement	May mitigate some transport issues, but performance depends on the application and environment
Key Use Cases	Enterprise networks and site-to-site connectivity	Remote access and secure communications via TLS	Simple, modern VPN tunnels	Applications and tunnels based on the QUIC transport protocol

The comparison presented in Table 1 demonstrates that the four technologies should not be regarded as directly interchangeable solutions. Each has distinct architectural characteristics that influence its suitability for different networking requirements. IPsec is commonly associated with network-layer protection and site-to-site connectivity, while TLS-based VPNs can be suitable for remote-access scenarios, depending on their implementation and configuration. WireGuard offers a purpose-built VPN architecture with a relatively streamlined design, whereas QUIC-based tunneling may be relevant to applications that benefit from QUIC's transport features, including connection migration under supported conditions.

Nevertheless, architectural differences alone are insufficient to determine which technology provides the best security or performance. Actual outcomes depend on implementation quality, cryptographic configuration, endpoint capabilities, network conditions, and deployment requirements. In particular, claims regarding throughput, latency, resource consumption, or comparative security should be supported by reliable published evidence or reproducible experimental measurements. Consequently, Table 1 should be interpreted as a qualitative technical comparison rather than as evidence of experimentally verified performance rankings. This distinction provides a basis for the subsequent discussion of the technologies' practical applicability and the limitations of the available comparative evidence.

3.4. Expected Outcomes

The aim of this concept paper on Virtual Private Networks (VPNs) is to give the following:

- In this paper a historical review will be provided concerning the history of this technology since its inception up to today. This paper will also discuss the impact this technology continues to have on today's network environments.
- The security, the performance of the VPNs and their fitness to various applications are all considered.
- VPN in today's networking environment: To allow the user to access the network remotely; To create a link between two different locations (site-to-site); and To secure applications hosted on the cloud.

- Identify issues and/or concerns that must be addressed before using and managing virtual private networks (VPNs) with your existing organization's network infrastructure; and create a structured approach to address these issues.
- In other words, if an organization has a secure, reliable and stable organizational network, then an organization can take advantage of all the benefits of using a VPN.

The way businesses are implementing a Virtual Private Network (VPN), security protocols and how they're using them will make it easier for businesses to make their network systems more secure and make the systems work better at the same time.

3.5. Challenges and Barriers

The biggest issue with the advanced technologies of VPNs is that there is always a new problem that has to be addressed. (Ostroukh et al., 2024; Tyshchenko et al., 2024). A variety of attacks can be made against VPN communication that could break the integrity or privacy of the communication. These are just a few of the many: vulnerabilities in the VPN protocols, misconfiguring VPN, and increased cyber attack risk. (Hritcan et al., 2025; Onesi-Ozigagun et al., 2024a). Moreover, the latency introduced in transferring the data due to the encryption and tunneling procedure makes it difficult to optimize the performance of the network and increase the security level.

The installation of VPN in enterprise and/or cloud based environment can be extremely complex (Amoo et al., 2024a; Zela et al., 2024). But, VPN installations do not seem to be the most suitable option for networks/applications that demand real-time data transmission because of the latency and processing overhead caused by the installation, and may even impact the performance of the system during peak demands (Mohamed & Kurnaz, 2024; Osasona et al., 2024). VPN installations can be integrated in the existing network infrastructure and security systems in various ways and are hard to implement on their own as well. Apart from that, other factors like firewall and router restrictions and compliance with regulations such as GDPR, HIPAA, PCI DSS will be important in the successful installation of a VPN (Hassan et al., 2024; Wang et al., 2024). Organizations should make sure that their installation of VPN is compliant with data protection/privacy regulations in multiple industries/jurisdictions. Lastly, the effect of VpNs on the user experience (speed and usability) should be taken into account (Chen et al., 2024)." VPN installations should enable users to have a secure and seamless experience — whether they are at home or on a mobile device — according to Chen et al. (2024) and Kjorveziroski et al. (2024). The cost of VPN implementation/ maintenance (Atadoga et al., 2024b; Ogundipe et al., 2024) is another important factor to consider when deciding on using a VPN.

The organizations should be able to afford the cost of implementation of VPNs. To address the issues outlined above through the use of VPNs, it is essential that an organization develop a VPN implementation plan, execute the plan as outlined and conduct regular monitoring of the plan for any issues that may arise with the VPNs (Amoo et al., 2024b; Onesi Ozigagun et al., 2024b). By choosing the best VPN deployment for their organization, tweaking the security policies when necessary, and staying ahead of the curve on threats and vulnerabilities, organizations can ensure that they have a secure and stable VPN solution.

4. METHODOLOGY

This paper on virtual private network (VPN) will consist of a detailed analysis of the existing study, scholarly papers, industry reports and examples on how the VPNs have been used in modern network architectures.

The basic steps of this framework are as follows.

- **The literature review":**The bulk of my paper will consist of a detailed review of each and every academic and commercial literature regarding Virtual Private Network (VPN) technology, Domain Name Protocol (DNP) technology and where both those technologies are headed. All types of documents, research papers, conference papers, academic papers and industry reports will be included.
- **Determination Of Important Subjects:** Consider the most important issues you will need to cover in your concept paper, including the development of VPN technologies; ways in which different types of security protocols can be applied to VPNs; what is currently being done with VPNs in networks; issues that arise when installing and using a VPN; and perhaps what the future of VPN technology might look like.
- **Data Collection:** Research all facts, statistics, case studies etc., etc., that relate to each of the main issues that you have identified. The resources could come from the World Wide Web, or from scholarly publications, trade and official documents of a VPN provider or other organization.
- **Synthesis and Analysis:** All the data collected should be analysed and brought together to impart an understanding of each of the major areas. Discuss various explanations of various types of security protocols that might be used in a VPN; discuss how VPN technology is used in real world scenarios; discuss any obstacles or considerations covered for implementing or maintaining a VPN.
- **Case studies and real-world examples**: Case studies and real-world examples will be provided to illustrate examples of how technology and security techniques do and do not work with VPNs in actual network environments. Talk about their experience with other businesses/organizations solving their problems using VPN solutions.
- **Conclusions**: The conclusion should also summarise the key points in the concept paper and

make conclusions based on a comparison. The conclusion should also highlight the significance of VPN technology, security protocol and its use in the current network configurations and what can be expected in the future in terms of developments in VPN technology. The concept paper, therefore, provides a comprehensive overview of VPN technology, security protocol, and how they can be applied in the present network environments to help organizations to design, deploy and manage VPNs successfully.

4.1. Strategies For Implementation

This paper introduces the concepts of Virtual Private Networks (VPNs) and will explain how these concepts can be used: The most crucial of the steps involved in conducting the study and analyzing the VPNs is:

- Identify all of the major topics you will write about in your concept paper: "Determine your goal(s) for your concept paper. This should be done by listing all major topics that you are going to write on (e.g. Advancements in VPS technology, Security requirements for VPS, Current usage of VPS in networks, etc.).
- Literature Review: "Search and gather the relevant information and views from the education-based literature as well as industry-based literature is essential to build the base for your research. Information gathered could then be utilized for your analysis and discussion of the concept paper.
- Data Collection: "I will gather the necessary data on VPN technology, security protocols and existing applications in today's network. All data gathered should be "valid, accurate and timely.
- Once you have gathered the data that will help you formulate your hypothesis, you need to merge and analyze the data you've gathered to find the most important trends, issues or concerns around the use of VPN technology. You should be able to describe how different kinds of security protocols can be used together with VPN technologies; in addition, how VPN technologies can be used as examples to explain how these technologies can be used. Also, provide examples of the application of VPN technologies to real world situations.
- The Case Studies are Real World Examples of how Companies can take Action in their Networks today, by incorporating VPN Technologies and VPN Security Practices, to solve Networking issues. Let's have a look at how organisations are employing VPNs to deal with some of the issues.
- In the discussion/recommendation section of the study, you will get to discuss your findings from the literature search and data collection/analysis. In this section of the paper you will be able to elaborate on how the information that you found in your research could be used in any business/organization that uses VPN technology to enhance business operation. Last but not least, you can suggest methods to organisations that are using VPN technology on how they can achieve better results, based on the results of your study.
- Based on the review of the concept paper, you can create a summary of the important results/key points included in the concept paper. The intent of this portion of the paper is to outline a few of the most important aspects associated with VPN technology such as the security protocols employed by VPNs, how VPNs are being integrated into the current network architectures, and possible future developments, trends or directions of VPN technology.

Implementing the concept paper in this implementation plan will help to assess technical and security aspects of Virtual Private Network (VPN) technology and security protocols. The evaluation will also explain the use of these technologies in today's network. Further, current VPN technology will be discussed as advantages and disadvantages of this technology will be addressed in this implementation plan. Finally, this implementation plan will suggest those organizations, which might need to use VPN technology.

4.2. Proposed Model

In this current research paper we will be looking at VPNs, the security protocols that a VPN can use and how they can be applied to today's networking environment. By understanding VPNs as a unique aspect of digital security and as the necessary component to network communications in today's world, we were able to create our concept. The first part of this chapter will be dedicated to understanding why VPNs are used – and why they are increasingly gaining in popularity. Moreover, at the beginning of this chapter you will learn how to make sure that your data isn't transmitted via the Internet to anyone else's sight or revelation. Also the evolution of VPNs from its early days till the current technology will be discussed in the first part of this chapter. To give an overview of both the development of the VPN technology and the history of them, the first part of this chapter will be dedicated to providing an overview of the VPN technology's history. Nowadays, there are lots of VPN technologies available. The different types of VPNs – Remote Access VPNs, Site-to-Site VPNs and Cloud Based VPNs – will be introduced and explained, and the reasons for their creation to address the needs of the current network architecture. As we focus on the development of VPN technology and the numerous configurations and applications of VPN technology in today's networks, we can start to understand the development of this technology. The first part of this section will outline some of the more popular security protocols used in (typical) implementations of VPNs, having succinctly outlined the evolution of VPN technology. IPSec, SSL/TLS, WireGuard and QUIC are included among the most widely used security protocols that will be described and examined in this section, which

will be divided into two parts: the first half will describe some of the most commonly used security protocols examined and described, while the second half will provide a brief overview of the cryptographic principles used to establish secure communications. The latter two security protocols, listed below, are still in use today, whereas the former two will be discussed in the second half of this section that will focus on the way that QUIC will be used to protect data transmission. If a VPN service uses none of the aforementioned security protocols, it will not be able to protect against unauthorized access to sensitive information, eavesdropping or tampering with data sent. In this section a few of the common and effective VPN implementations will be explained. The first part of this section will also focus on the need to select the right security technologies to ensure that maximum performance and reliability is achieved when deploying VPNs in different network architectures. The goal of the first half of this chapter is to put together a framework of thoughts to consider the way VPNs might be developed and how they can be used to defend modern networks, where and when. As a reminder to all of you, in this connected world it's important to take steps to make communications and personal privacy secure, using a VPN and security measures. The conceptual paper will be an introduction to several of the more common protocols that can be used to create a VPN (IPSec, SSL/TLS, WireGuard, QUIC) and then the paper will discuss each of these protocols individually and critically, including its security features, performance and applicability in different scenarios. This last portion of the document (section 3), will outline the pros and cons of each protocol in relation to each threat or attack against network security or performance. They are now being implemented with Virtual Private Networks (VPNs) and the use of this network will be covered in this document. The focus of this discussion will be on the security issues surrounding cloud services, site-to-site connectivity and remote access. Examples/real life use cases / case studies will be used to show the pros/cons of using a VPN in the real world. Real life examples/applications will be provided to illustrate some of the ways that many different types of organizations can be effective utilizing VPNs. In addition, some of the big challenges that are encountered in the current network environment in relation to the deployment / maintenance of VPNs will be highlighted. The above issues will be discussed and solutions to issues will be suggested in the document and the scalability issues and integration of VPN system with other systems will be included. Some organisations will be given some suggestions as to how to address these concerns. The idea here is that organisations can apply the model suggested in this document to make future deployments/administrations of VPN more effective to meet network requirements of organisations. Lastly, future trends/emerging technologies which will impact on the trajectory of VPNs will be explored. Other areas gaining traction are the use of machine learning and artificial intelligence (AI) as tools to improve performance of VPNs, and the growing significance of the role of VPNs in IoT/edge computing. The trends that are emerging will be discussed in detail to understand their implications on network performance and security and the possibility of future evolution to meet the future networks' requirements. At the end of this conceptual paper a framework will be provided to assess VPN technology/security-protocols and how they are used in today's networks. It will suggest ways to deploy a VPN solution that meets the requirement of the companies to operate within the limits of community security and maximise efficiency.

4.3. The Model

The aim of this conceptual paper is to create a conceptual framework that will help to explain and analyse the elements of Virtual Private Networks (VPNs) as well as the use of these elements in the current network environment. Pillar "1": This pillar will address the evolution of the technology of the VPN and how it came to its current place. It will also cover some VPN fundamentals and offer some final insights.
Next will be an overview of various types of Virtual Private Networks (VAN or Remote Access) Site-to-Site VPN and Cloud Based VPNs along with their advantages and disadvantages. In this course you will be introduced to the advantages/disadvantages of each type of VPN, and the procedures/processes that have been developed for keeping all data transmitted over a network confidential. We describe the various VPN solutions (IPSec, QUIC, SSL/TLS and WireGuard), their drawbacks/benefits, performance details and application scenarios. This section seeks to provide a clearer view as to how VPNs can be used to provide secure remote access to users, to connect sites together and to provide protection of cloud based services. It also provides an insight into "real world" and case studies demonstrating the use of VPN technologies to address real world networking challenges and to meet business objectives. This will be a part one of two on challenges/problems with deploying/managing VPNs in today's network environments: Part one will be challenges/problems, part two will be solutions/suggestions. With this model you can determine if you have some questions about your deployment of a VPN (such as is my VPN scalable? May I connect to my vpn using other systems? What are the rules to be followed if using a VPN? Then ask my users what they think of the use of the VPN (how, how often, etc.) and provide potential solutions to these problems to enhance your VPN deployment. By the end of this course, you will have a detailed understanding of VPN technology, security protocols and how they are used in modern day networking. A nice example of VPN evolution and a good illustration of the advantages/disadvantages of each of the different VPN protocols and reasons why an organization might select a specific protocol. You will also be provided with "best practices" or "deployment guides" which will help you deploy and manage your VPN to get the best results in terms of both security and performance. In conclusion,

this model is a more comprehensive view of the intricacies of VPN technology and its importance in maintaining the seamless flow of network communications in today's digital era.

4.4. The advantages and disadvantages

These reviews provide a lot of details with regards to the past endeavours and can be really useful in network security, updated network management and also for composing a conceptual record for a Virtual Private Network (VPN). I highly recommend that you read the review. The review also gives an in-depth knowledge of VPN technology and about the various kinds of security protocol employed in the implementation of VPNs, which can help organizations understand the worth of VPN technology in enabling them to conduct business communications via safe networks.

This concept paper aims to prove the usefulness of a vpn, to promote awareness and potentially to increase the number of users using a vpn to enhance the security of the networks they use to send/receive information. The concept paper also examines various types of VPNs available in the market today, and their application in the existing networks. Both the advantages and disadvantages of each type of VPN have been studied by analysts, enabling companies to choose the type of VPN solution with features appropriate for them. In making such informed decisions, networks will be more reliable, efficient and effective. Organizations will also gain the ability to eliminate the need for costly private dedicated networks or leased lines, and therefore reduce their infrastructure costs, while at the same time gaining insight into how organizations can save money by using VPNs. This concept paper is further evidence of the importance of decision makers to invest in VPN technology. Another important point that is discussed on this concept paper is on the topic of security/regulatory compliance. VPNs provide a way to become compliant with regulations; especially in areas of the business where data security is critical. As part of the organisation's compliance, if it relies on VPN, then the organisation will be able to maintain its operational capabilities and avoid non-compliance penalties/fines. VPNs provide an integral role in providing business continuity. With this one, VPNs enable remote workers to securely access corporate resources. The concept paper illustrates the remote access to critical resources from anywhere, anytime with the use of a VPN. This example is very applicable at present because how we conduct business has evolved from previous methods - specifically remote and digital.

The primary goal of this VPN Concept Paper is to provide a list of some of the basics that companies can take to make their networks more secure and efficient using VPN technology. With an understanding of the advantages of VPNs as well as some of the dangers that can occur if VPNs aren't managed appropriately, you can make a well informed decision on whether or not to incorporate VPNs into your company's network design. If you choose to use and retain VPNs in your network design, you are securing your company's network, complying with all the applicable government laws and ordinances related to network security, as well as saving money that otherwise could be spent on running your company.

5. CONCLUSION

The Virtual Private Network (VPN) Concept Paper gives details about every aspect of VPN. It also explains various types of security protocols used in VPNs and how VPNs can be incorporated into the existing networking technologies. VPN technology has developed several security protocols, each with its own set of characteristics, that offer security when using a network to send and receive data, such as IPSec, SSL/TLS, WireGuard and QUIC. VPN services are currently available to safely transfer information, join offices and secure Apps in the cloud. Data is sent over networks which may not be secure. It's, therefore, clear that VPNs are vital elements in today's network security. VPNs offer a lot of advantages. But, there are many drawbacks in the use of VPNs as well. Some of these are scalability limitations; compatibility limitations; and compliance limitations that will pose problems for organizations as they move to deploy VPNs. In this network environment, it is necessary to make the right plans and deploy the VPNs dynamically to effectively manage and use the VPNs.

Alternatively, you can choose a VPN technology that you want to carry out in the future. New technologies like VPNs and new technology (edge computing, IoT will provide new, improved security and functionality along with new machine learning and AI technologies. With the shift towards a fully-digital world, VPNs could well be an important part of the security equation for network communication for many years to come.

Lastly, there's a summary of the benefits of VPN technologies in the existing topology of a company's network. Also, the author suggests some recommendations and practical tips to organizations that would like to deploy VPN technologies to meet their organizational needs. Organizations will have high security level of communications over their network, and have a better network security posture when utilizing VPNs, once they understand the types of security protocols utilized by VPNs, and what type of applications can be run over VPNs.

References:

Ajala, O. A., Arinze, C. A., Ofodile, O. C., Okoye, C. C., & Daraojimba, O. D. (2024). Big data analytics in the age of high surveillance: activity report on the development of privacy-enhancing technologies, *World Journal of Advanced Engineering Technology and Sciences*, 11(1), 294-300.

Akinsanya, M. O., Ekechi, C. C., & Okeke, C. D. (2024). Virtual private networks (VPN): a conceptual review of security protocols and their application in modern networks. *Engineering Science & Technology Journal*, *5*(4), 1452-1472.

Alia, O., Huang, A., Luo, H., Amer, O., Pistoia, M., & Lim, C. (2024, March). Quantum-safe 10 Gbps site-to-site IPsec VPN tunnel over 46 km deployed fibre. In *Optical Fiber Communication Conference* (pp. Th3B-5). Optica Publishing Group.

Amoo, O. O., Atadoga, A., Osasona, F., Abrahams, T. O., Ayinla, B. S., & Farayola, O. A. (2024a). GDPR's impact on cybersecurity: A review focusing on USA and European practices, *International Journal of Science and Research Archive*, 11(1), 1338-1347.

Amoo, O. O., Osasona, F., Atadoga, A., Ayinla, B. S., Farayola, O. A., & Abrahams, T. O. (2024b). Cybersecurity threats in the age of IoT: A review of protective measures, *International Journal of Science and Research Archive*, 11(1), 1304-1310.

Atadoga, A., Farayola, O. A., Ayinla, B. S., Amoo, O. O., Abrahams, T. O., & Osasona, F. (2024a). A comparative review of data encryption methods in the Europe, *Computer Science & IT Research Journal*, 5(2), 447-460.

Atadoga, A., Osasona, F., Amoo, O. O., Farayola, O. A., Ayinla, B. S., & Abrahams, T. O. (2024b). The role of IT in enhancing supply chain resilience: a global review, *International Journal of Management & Entrepreneurship Research*, 6(2), 336- 351.

Ayinla, B. S., Amoo, O. O., Atadoga, A., Abrahams, T. O., Osasona, F., & Farayola, O. A. (2024). Ethical AI in practice: Balancing technological advancements with human values, *International Journal of Science and Research Archive*, 11(1), 1311-1326.

Bhagat, N. (2021). MPLS vs. IPsec VPN: Choosing the Right Network Architecture for Enterprise WAN. *International journal of scientific research in engineering and management*. *5*(12). *DOI: 10.55041/ijsrem11326*.

Chen, L., Xue, K., Li, J., Li, Z., & Yu, N. (2024, February). Security-enhanced Wire Guard protocol design using quantum key distribution. In *2024 International Conference on Computing, Networking and Communications (ICNC)* (pp. 718-723). IEEE.

Filipescu, A., Simion, G., Ionescu, D., & Filipescu, A. (2024). IoT-Cloud, VPN, and digital twin-based remote monitoring and control of a multifunctional robotic cell in the context of AI, industry, and education 4.0 and 5.0. *Sensors*, *24*(23), 7451.

Forbacha, S. C., & Agwu, M. J. A. (2023). Design and implementation of a secure virtual private network over an open network (Internet). *American Journal of Technology*, *2*(1), 1-36.

Fu, C., Wang, B., Wang, W., Mu, R., Sun, Y., Xin, G., & Zhang, Y. (2024). A generic high-performance architecture for VPN gateways. *Electronics*, *13*(11), 2031.

Gentile, A. F., Macrì, D., Greco, E., & Fazio, P. (2024). Overlay and virtual private networks security performances analysis with open source infrastructure deployment. *Future Internet*, *16*(8), 283.

Hassan, A. O., Ewuga, S. K., Abdul, A. A., Abrahams, T. O., Oladeinde, M., & Dawodu, S. O. (2024). Cybersecurity in banking: a global perspective with a focus on Nigerian practices, *Computer Science & IT Research Journal*, 5(1), 41-59.

Hritcan, D. F., Graur, A., Balan, D. G., & Timofte, E. M. (2025). A performance analysis of VPN technologies used in an IoT environment. *Advances in Electrical and Computer Engineering*, *25*(2), 81-88.

Jevremovic, A., Kostic, Z., Chorbev, I., Perakovic, D., Shalaginov, A., & Cvitic, I. (2024). Energy efficiency of kernel and user space level VPN solutions in AIoT networks. *IEEE Open Journal of the Computer Society*, *6*, 199-210.

Jumakhan, H., & Mirzaeinia, A. (2023, December). Wireguard: An Efficient Solution for Securing IoT Device Connectivity: Regular Research Paper (CSCI-RTMC). In *2023 International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 934-940). IEEE.

Kjorveziroski, V., Bernad, C., Gilly, K., & Filiposka, S. (2024). Full-mesh VPN performance evaluation for a secure edge-cloud continuum. *Software: Practice and Experience*, *54*(8), 1543-1564.

Kosanam, A., Ayalasomayajula, N., Vivek, G., & Kavitha, C. R. (2024, November). Enhancing Web Security with Two-Way Authenticated SSL Communication. In *2024 8th International Conference on Electronics, Communication and Aerospace Technology (ICECA)* (pp. 496-500). IEEE.

Lafourcade, P., Mahmoud, D., & Ruhault, S. (2024). A unified symbolic analysis of wireguard. In *Usenix Network and Distributed System Security Symposium*.

Manulal, M. (2024). Enhancing Data Security with WireGuard: A Comprehensive Study. *Journal of Network & Information Security*, *12*(1), 14.

Mishko, O., Matiuk, D., & Derkach, M. (2024). Security of remote iot system management by integrating firewall configuration into tunneled traffic. *Вісник Тернопільського національного технічного університету*, *115*(3), 122-129.

Mohamed, S. A. A., & Kurnaz, S. (2024). Classified VPN network traffic flow using time related to artificial neural network. *Computers, Materials & Continua*, *80*(1), 819-841.

Ogundipe, D.O., Odejide, O.A., & Edunjobi, T.E (2024). Agile methodologies in digital banking: theoretical underpinnings and implications for custom satisfaction, *Journal of Science and Technology*, 10(02), 021-030.

Ogungbemi, O. S., Ezeugwa, F. A., Olaniyi, O. O., Akinola, O. I., & Oladoyinbo, O. B. (2024). Overcoming remote workforce cyber threats: A comprehensive ransomware and bot net defense strategy utilizing VPN networks. *Available at SSRN 4911878*.

Onesi-Ozigagun, O., Ololade, Y. J., Eyo-Udo, N. L., & Ogundipe, D. O. (2024a). Leading digital transformation in non-digital sectors: a strategic review, *International Journal of Management & Entrepreneurship Research,* 6(4), 1157-1175.

Onesi-Ozigagun, O., Ololade, Y. J., Eyo-Udo, N. L., & Ogundipe, D. O. (2024b). Revolutionizing education through AI: a comprehensive review of enhancing learning experiences, *International Journal of Applied Research in Social Sciences,* 6(4), 589- 607.

Osasona, F., Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. A., & Ayinla, B. S. (2024). Reviewing the ethical implications of AI in decision making processes, *International Journal of Management & Entrepreneurship Research*, 6(2), 322-335.

Ostroukh, A. V., Pronin, C. B., Podberezkin, A. A., Podberezkina, J. V., & Volkov, A. M. (2024, July). Enhancing Corporate Network Security and Performance: A Comprehensive Evaluation of WireGuard as a Next-Generation VPN Solution. In *2024 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)* (pp. 1-5). IEEE.

Patil, V., & Korde, S. (2018). Protocols for Virtual Private Networks. *International Journal of Emerging Technology and Computer Science*, *3*(4), 16-22.

Ramly, A. M., Ng, Z. W., Khamayseh, Y., Kwan, C. S. C., & Neo, T. K. (2024). Review and enhancement of VoIP security: Identifying vulnerabilities and proposing integrated solutions. *Journal of Telecommunications and the Digital Economy*, *12*(4), 109-136.

Saad, M., Ahmed, W., & Khan, M. M. (2024, November). Design and analysis of quantum safe virtual private network. In *2024 4th International Conference on Innovations in Computer Science (ICONICS)* (pp. 1-8). IEEE.

Sharma, K., Tahiliani, M. P., & Rathod, V. J. (2024, July). Design and development of an emulation model for VPN and VPN bonding. In *2024 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)* (pp. 1-6). IEEE.

Shim, H., Kang, B., Im, H., Jeon, D., & Kim, S. M. (2025). qTrustNet virtual private network (VPN): Enhancing security in the quantum era. *IEEE Access*, *13*, 17807-17819.

Tian, Y., Cao, Z., & Huang, S. H. S. (2024, October). Detecting VPN Traffic in Real-Time with Active Probing. In *2024 22nd International Symposium on Network Computing and Applications (NCA)* (pp. 132-139). IEEE.

Tymoshchuk, V., Karnaukhov, A., & Tymoshchuk, D. (2024). USING VPN TECHNOLOGY TO CREATE SECURE CORPORATE NETWORKS. *Collection of scientific papers «ΛΌГОΣ»,(June 21*, 166-170.

Tyshchenko, D., Franchuk, T., Zakharov, R., & Moskalenko, V. (2024). Supporting dynamic security needs with VPN tools. *Системи управління, навігації та зв'язку. Збірник наукових праць*, *3*(77), 149-152.

Wang, C., Yin, J., Li, Z., Xu, H., Zhang, Z., & Liu, Q. (2024, May). Identifying vpn servers through graph-represented behaviors. In *Proceedings of the ACM Web Conference 2024* (pp. 1790-1799).

Zela, D., Mema, B., & Zela, K. (2024). VPN virtual private network applications in data prediction. *Smart Cities and Regional Development (SCRD) Preprints*, *1*(1).

Israa Chyad
University of Sumer,
Iraq.
Asraaadnan74@mail.com
ORCID: 0009-0003-6541-9726