Vol. 2 No. 5 (2024)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

Critical Evaluation of Data Privacy and Security Threats in Federated Learning: Issues and Challenges Related to Privacy and Security in IoT

Mehwish[1]*

Department of Software Engineering, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan. Corresponding Author Email: SU92-MSSEW-S24-001@superior.edu.pk

Mahnoor Zaheer[2]

Department of Software Engineering, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan

SU92-MSSEW-S24-003@superior.edu.pk

Muhammad Hamza Azeem[3]

Leopold-Franzens-Universität Innsbruck.

hamzaazeem990@gmail.com

Zain Afzal[4]

Faculty of Mathematics, Computer Sciences and Physics, Leopold-Franzens-Universität Innsbruck, 6020, Innsbruck, Austria.

zainafzal26@hotmail.com

Hafsa Karim[5]

Tech university of Korea. hafsarao27@gmail.com

Hamayun Khan[6]

Department of Computer Science, Faculty of Computer Science & IT Superior. University Lahore, 54000, Pakistan

hamayun.khan@superior.edu.pk

Abstract

Data security and privacy received a great deal of research attention recently, as privacy protection becoming a key factor in the development of artificial intelligence based IOTs. The End-to-

Vol. 2 No. 5 (2024)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

End VPN security has an essential role especially in connecting smart objects in the Internet of Things (IoT) environments. It noted that security is a crucial issue in the End-to-End VPN approach. The application of Machine Learning (ML) techniques to the well-known intrusion detection systems (IDS) is key to cope with increasingly sophisticated cybersecurity attacks through an effective and efficient detection process. This paper provides a comprehensive exploration of Virtual Private Network (VPN) technologies, emphasizing their importance in modern networking for ensuring secure communication over untrusted networks like the internet. VPNs have evolved significantly, addressing the growing need for data protection in both personal and enterprise contexts. This study delves into various VPN protocols such as PPTP, L2TP/IPsec, OpenVPN, IKEv2/IPsec, and WireGuard, evaluating their security mechanisms, strengths, and vulnerabilities. The paper also examines the emerging challenges facing VPNs, including advanced cyber threats and the impact of evolving technologies such as quantum computing. Furthermore, the study highlights future directions, such as integrating AI for dynamic threat detection and developing quantum-resistant VPN protocols. Through this analysis, the aim is to provide actionable insights into optimizing VPN usage for enhanced network security in an increasingly complex digital landscape.

Keywords: VPN, Security Protocols, Encryption, OpenVPN, IKEv2/IPsec, WireGuard, Quantum Computing

Introduction

Modern IT infrastructures can cover large geographic areas, and therefore, secure and reliable IT infrastructures are needed, while also guaranteeing low-cost factors, both in terms of space and

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

time. The virtual private network (VPN) is one of the most reliable technology to satisfy this type of need, passing both through the "old" (PSTN) and through the most modern 4G/5G architectures [1]. A Virtual Private Network (VPN) creates a secure connection between a user's device and a remote server, ensuring privacy and data integrity over public networks. This is achieved through tunneling protocols, encryption standards, and robust authentication mechanisms [2]. As cyber threats become increasingly sophisticated, understanding the role of VPNs in mitigating these risks is critical. This paper explores the technological evolution of VPNs, examines their contemporary applications, and identifies potential advancements to address emerging security challenges [3].

The Internet of Things (IoT) has achieved great popularity and acceptance with the rapid growth of high-speed networks and smart devices. In this respect, IoT represents a network, in which "things" or devices are interconnected through a public or a private network [4, 5]. These devices are equipped with tiny sensors and powerful hardware that collect and process data at unprecedented speed Researchers have explored various approaches to address these concerns, including the development of lightweight cryptographic algorithms to secure data transmission and storage in resource-constrained IoT devices. Additionally, efforts have been made to design secure frameworks and authentication protocols to mitigate the risks of IoT-related security breaches. Another key challenge in the IoT domain is the protection of user privacy [6, 7]. As IoT devices collect and transmit vast amounts of personal data, there is a growing concern about the potential misuse of this

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

information, such as unauthorized surveillance, profiling, and targeted advertising [8, 9].

Federated Learning

The general framework of FL consists of multiple clients and a cloud server, where each client downloads a shared global model from the cloud server for the local training of data. Afterward, all of the clients periodically forward their locally trained models to the cloud server [10, 11]. The cloud server performs a global average and aggregates the improved global model to the clients. This communication between the clients and the cloud server (usually known as communication round) is continuously repeated until the desired convergence level is achieved [12, 13]. The data distribution among clients in FL further classifies it into three categories; Horizontal Federated Learning (HFL), Vertical Federated Learning (VFL), and Federated Transfer Learning (FTL) [14]. Below, we define general framework from security perspectives:

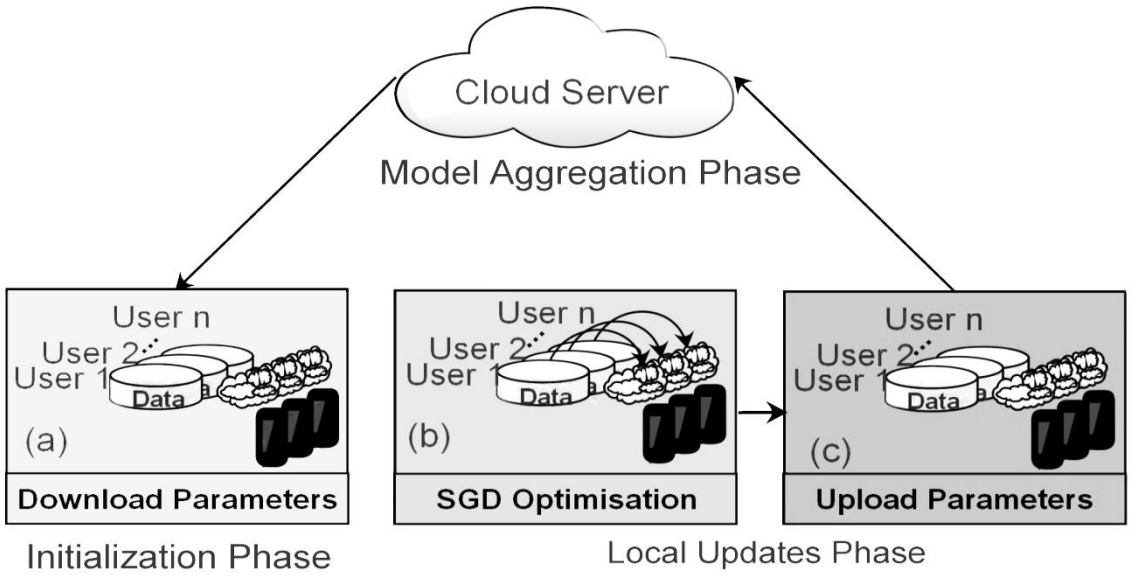

Figure 1: Federated learning Framework [15]

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

In realistic scenarios, the latency of inferring directly from participants is much lower communication than predicting in the cloud and then transferring to participants [16]. The implementation of FL in mobile edge networks accelerates content delivery and improves mobile service quality by reducing unnecessary system communication load . The model inference is completed locally without a cloud round-trip that avoids propagation delay caused by transferring data, and thus latency-sensitive applications can benefit from such a solution [17, 18]. A virtual private network (VPN) connection is a secure method of transmitting private data through a dedicated private circuit.

Table 1: Comparative Analysis of Security Protocols [19]

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

Literature Review

VPNs are indispensable tools in today's digital ecosystem, serving as safeguards for personal privacy, enterprise data security, and secure communication in remote work settings. They ensure confidentiality, integrity, and authentication, enabling secure transmission of sensitive information. Moreover, VPNs are instrumental in circumventing geo-restrictions and ensuring internet freedom, particularly in regions with stringent censorship

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

laws [20- 23]. 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 [24-27].

Figure 2: Virtual private network Tunnelling from LAN1-LAN2 [28]

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 [29, 30]. 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 [31, 32] 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. Below mentioned Table 2 represents Security Protocols Findings They have shifted from simple remote access

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

tools to essential security technologies, helping protect users and organizations from a growing array of cyber threats [33-35].

Vol. 2 No. 5 (2024)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

Table 2: Security Protocols Finding [36]

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

Materials

The rapid proliferation of the Internet of Things has brought about a significant transformation in the way we interact with our surroundings, but with this innovation comes a critical set of challenges related to data privacy and security. As the number of interconnected devices continues to grow, the potential for malicious actors to compromise sensitive information and disrupt critical systems has become increasingly concerning. One of the primary issues in the IoT landscape is the inherent vulnerability of these devices, which are often designed with limited security measures and lack robust authentication mechanisms. The ease of accessibility and the direct interaction with the physical world make IoT devices an attractive target for cyber-attacks, exposing users to a range of threats such as data breaches, unauthorized access, and even physical harm.

PPTP Security Protocol

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

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

security flaws, particularly with weak encryption. As a result, it couldn't offer the level of protection needed for sensitive data.

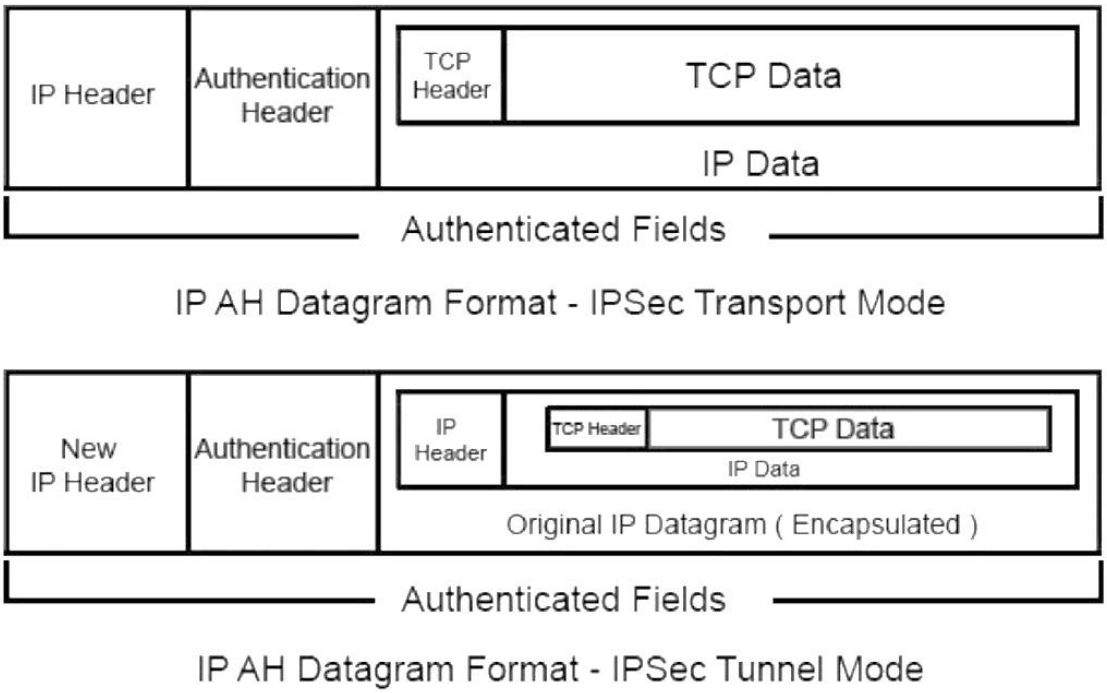

Figure 3: VPN based IPSec [37]

Cryptography Techniques (CT)

The cryptography techniques, such as homomorphic encryption and secure multi-party computation (SMC), are widely used in the existing literature of privacy-preserving FL algorithms. In particular, each client encrypts the update before uploading it to the cloud server, where the cloud server decrypts these updates in order to obtain a new global model [38]. However, these techniques are vulnerable to inference attacks, because each client has to share the gradients accessible to the adversaries. Applying cryptography techniques to the FL systems can also result in major computation overhead, due to the extra operations of encryption and decryption. Figure 4 shows how Plain texst to Codeword

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Conversion using Cryptographic Algorithms for Data Traffic Security [39, 40].

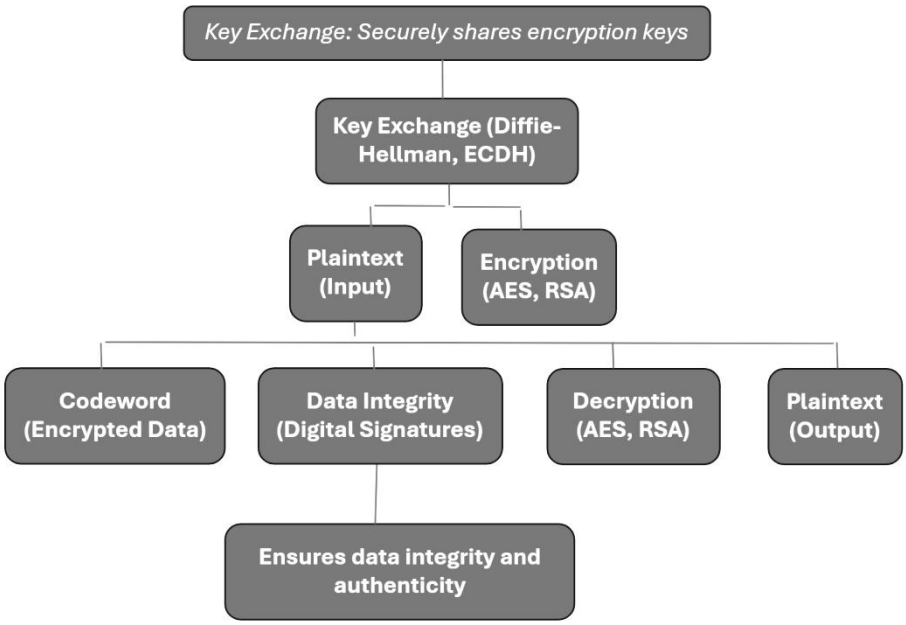

Figure 4: Plain text to Codeword Conversion using Cryptographic Algorithms for Data Traffic Security [41].

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 [42, 43].

Security Challenges Facing VPNs

Evolving Cyber Threats: Modern attackers employ sophisticated techniques, such as advanced persistent threats and zero-day vulnerabilities, to compromise VPN connections [44].

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Quantum Computing Risks: Future quantum computers could render current encryption algorithms obsolete, necessitating the development of quantum-resistant protocols [45, 46].

Performance Overhead: Balancing robust encryption with minimal latency remains a challenge, particularly for high-traffic environments. Considering this below figure represents the two modes Network Security Protocols (a) Transport mode (b) Tunnel mode.

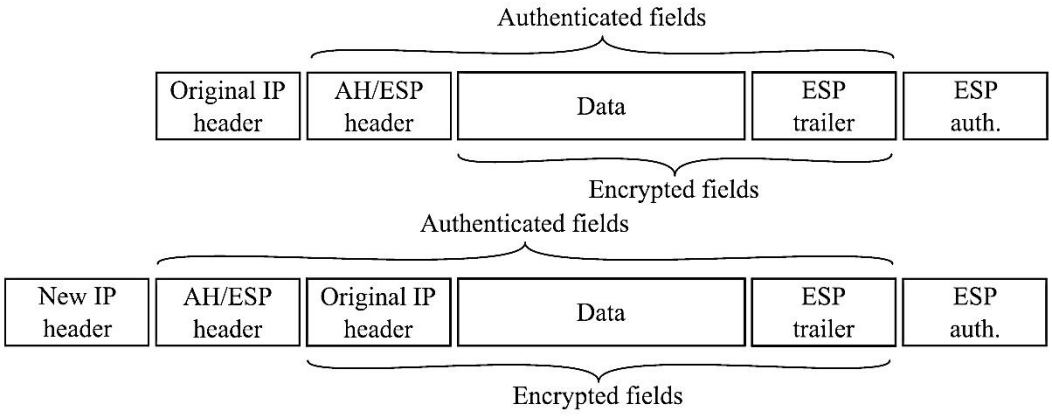

Figure 5: Network Security Protocols (a) Transport mode (b) Tunnel mode [47]

Emerging Solutions and Future Directions

1. AI Integration: Leveraging artificial intelligence for real-time threat detection and adaptive security configurations. Post-Quantum Encryption: Developing VPN protocols that resist quantum-based attacks.

2. Edge Computing and IoT: Enhancing VPN compatibility with resource-constrained devices in edge networks. This study synthesizes insights from recent international research and practical case studies. Performance and security evaluations of VPN protocols were conducted using real-world scenarios, network analysis tools, and surveys with cybersecurity professionals.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

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 [49, 50]. 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 [51, 52]. 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 [53, 54]. 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 [55, 56].

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

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 [57].

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. 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.

Challenges and opportunities in FL over wireless network

In federated learning, local models are trained on end-devices and then combined on a central server. The global model is continuously sent back to end-devices until convergence is

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

achieved. Federated learning relies on iterative interaction between end-devices and the aggregation server, necessitating efficient optimization schemes like FedAvg and FedProx. Subsequently, the aggregated weights (global model) are returned to the end-devices. Despite its benefits, federated learning encounters challenges such as privacy issues, resource optimization, incentive mechanisms, and statistical and system heterogeneity

Conclusion and Recommendations

In this paper, we presented an overview of current approaches for the classification and analysis of encrypted traffic, federated learning specially virtual private network. First, we selected a number of the most widely used encryption protocols and described their packet structure and standard behavior 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 VPNs are critical for maintaining secure communications in the modern digital landscape. However, their effectiveness depends on staying ahead of emerging threats and adopting innovative solutions. Key recommendations include:

- Transitioning to quantum-resistant encryption algorithms.
- Integrating AI for adaptive and proactive security measures.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

- Optimizing protocols like WireGuard for broader compatibility and performance

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

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

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

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.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[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

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[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 (Al) and Blockchain-Based

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

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

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[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

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[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

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

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.

[52] Zscaler. (2024). VPN Risk Report: Over Half of Organizations Experienced VPN-related Cyberattacks. Retrieved from https://www.zscaler.com/press/vpn-risk-report-finds-more-half-organizations-experienced-vpn-related-cyberattack-last-year

[53] MDPI. (2024). Zero Trust VPN: A Systematic Literature Review. Information, 15(11), 734. Retrieved from https://www.mdpi.com/2078-2489/15/11/734

[54] DiVA Portal. (2024). VPN Performance and Configuration Challenges. Retrieved from https://www.diva-portal.org/smash/get/diva2%3A1778036/FULLTEXT03.pdf

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[55] ArXiv. (2024). WireGuard and IoT Security: Evaluations and Perspectives. Retrieved from https://arxiv.org/abs/2402.02093

[56] ArXiv. (2024). DoS Vulnerabilities in VPNs: Analysis and Countermeasures. Retrieved from https://arxiv.org/abs/2110.00407

[57] ArXiv. (2024). Security Analysis of Proprietary VPN Clients. Retrieved from https://arxiv.org/abs/2202.05573