Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Systematic Literature Review on VPN Security: Adaptive Multi-Tunnelling as a Mitigation Strategy

[1]Mrs.C. Deepika, [2]Dr. K. Abirami
[1]*Ph.D. Research Scholar, school of Computing Sciences, Department of Computer Science, Chennai*
Email: deepika2303deepi@gmail.com
[2]*Assistant professor, School of Computing Sciences, Department of Computer Sciences, Vels University, Chennai*
Email: abiramidharmarajan@gmail.com

ARTICLE INFO

Received: 26 Dec 2024

Revised: 14 Feb 2025

Accepted: 22 Feb 2025

ABSTRACT

In recent years, virtual private network provides a private and secure network architecture for individuals and organizations by using with the support from Internet. VPN helps in safe data transmissions without the need for dedicated physical connections, allowing to creation of a secure communicational channel between remote users, sites, and corporate offices. The proposed research focused on exploring a systematic literature review on VPN security concerning adaptive multi-tunnelling as a mitigation strategy. The systematic review adopted PRISMA framework to minimizing bias and ensuring the transparency of the survey. The survey used various databases such as Google Scholar, Research Gate, and Scopus were used to collect the research articles published from 2018 to 2025. The keywords used "corporate cybersecurity", "adaptive security mechanisms," "multi-tunneling VPN," and "VPN security".11 articles were included for final inclusion of the research. The major themes identified in the research are multi-tunnel architecture and deployment models, traffic splitting and load balancing mechanisms encryption and key management strategies and network adaptation and dynamic routing. The implementation of traditional VPN security was enhanced with adaptive multi-tunneling. The major issues associated with VPN, such as mitigation, scalability, and resilience, were addressed by the adaptive multi-tunneling technique. The adoption of adaptive multi-tunneling in VPN security gained a significant advantage in mitigating vulnerabilities and optimizing performance in mobile networks. Potency, latency, and computational overhead were considered major disadvantages in implementing adaptive multi-tunneling in VPN security.

Keywords: VPN Security, Adaptive Multi-Tunnelling, Mitigation Strategy, Adaptive Security

1. INTRODUCTION

A virtual private network (VPN) can provide a private and secure network architecture for individuals and organizations by using the Internet. The VPN's secure, cost-effective, and reliable services are considered significant, ensuring wide implementation in the networking and telecommunications sector. The integration of VPNs prevented the expensive usage of the Internet in the IT sector helps to reduce infrastructure costs by utilizing the public internet. VPN achieved safe data transmissions without the need for dedicated physical connections, allowing to creation of a secure communicational channel between remote users, sites, and corporate offices.

The tunneling protocol supported various VPN functionality and provided a secure mode of network services (Akter et al., 2022). Nearly 2365 types of cyber-attacks were targeted by 343,338,964 people in the year 2023 (Ghelani, 2022; Kaur & Ram Kumar, 2022).By using email, 96% of phishing attacks were delivered (Alkhalil et al., 2021). Additionally, major challenges in the cyber-attack were caused by ransomware, expected to climb nearly USD 265 billion by 2031 annually (McIntosh et al., 2022). The appropriate mitigation strategies need to be identified to help protect an organization with an understanding motives behind the attack (Fatima et al., 2021).The legitimate user was blocked from accessing resources or services on a network by a denial of services attack (Streun et al., 2022; Zhou & Zhang, 2020).

1.1 Understanding Virtual Private Networks (VPNs)

Most companies rely on remote work technology and various technologies to access the organizational network. VPN assures the safe transfer of data between remote locations by encrypting the information during transmission.

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Secure data transfer with VPN is ensured with SSL, which helps users connect with a web browser and operates at the application layer. The transport-level secretary in the VPN network is managed efficiently by cryptography and provides encrypted public keys for authentication. The connection between the client and the resource was managed by encrypting data in transit.

1.2 Security Challenges in VPN Architecture

Security limitations and implementation challenges impacted the widespread usage of VPNs. Unrestricted access to the network by VPN causes significant issues by assuming all users are trustworthy in turn causes major security risks. To ensure safe and smooth access, VPN users need to choose the most secure and reliable VPN solutions (Bansode & Girdhar, 2021; Sawalmeh et al., 2021). The protected virtual network using VPN was created by using encryption and tunneling protocols (Zohaib et al., 2024). The VPN connected geographically helps to ensure secure remote access by managing privileges and maintaining the integrity of data. On the other hand, the traditional telecom architecture was significantly impacted by a hardwired network and physical configuration assured with security parameters helps to keep up with the evolving nature of cyber threats (Abbas et al., 2023).

1.3 Evolution of VPN Technologies

The historical development of VPN technology from the 1970s to the 1980s traces its origin to virtual circuit technology. Between the source and destination port, a logical path was established using a virtual circuit over a shared network. By using multiple routers, actual data was transferred to the network. The security in the VPN network was enhanced with the integration of encryption techniques, integrated with virtual circuit technology helps to improve security. Moreover, the security measures in VPN were strengthened with the use of an advancement in token authentication. The challenges caused by cyber threats in traditional communication lines were addressed with the introduction of VPN helps to provide secure communication over public networks by encrypting data and implementing authentication mechanisms (Jyothi & Reddy, 2018).

2. THE NEED FOR ADAPTIVE MULTI-TUNNELLING

Over a network, data packets were transferred using the tunneling technique in the network. In the transport network, the original data packet with the integration of the protocol was not supported by the host network, was encapsulated with another packet, and transmitted with the help of the VPN network. VPNs use the technique of tunnelling to transfer the original data packets. Various types of tunneling, such as full tunneling and split tunneling, shift to zero trust security model. The remote connection in the network was supported with VPN by the zero-trust approach helps to ensure data security and privacy. The complete security and encryption in the VPN network were assured with the implementation of full tunneling helps to route through the VPN tunnel (Harmening, 2025a)

2.1 Limitations of Traditional VPN Tunnelling

The implementation of the traditional VPN tunneling mechanism caused several security and performance issues. The major challenge was caused due to the dependency of a single tunnel used by VPN to transmit data. The occurrence of traffic correlation and man-in-the-middle attacks was considered vulnerable to targeted attacks caused by traditional VPN tunneling. Additionally, the challenges caused by encryption in traditional VPN protocols were addressed by the adoption of the zero-trust model helps protect data and ensure privacy (Elavarasan et al., 2024). Due to a limited number of available Internet Protocol address space, the protocol was replaced with version 6 was considered a replacement for IPv4 (Harmening, 2025b). The insider threat risk was increased due to the grant of unrestricted access to the network adopted by the traditional VPN network. The continuous authentication and granular access control challenge exists in the zero-trust VPN framework

2.2 Multi-Tunnelling as a Resilient Security Strategy

The implementation of a complex algorithm was needed to prevent and security of user data in the VPN header to avoid the tampering of data. The data transfer features reliable data transfer through the use of different encryption algorithms in multiple levels and multiple times. Multi-tunneling features were adopted in order to increase VPN security and use more than one encrypted tunnel to keep the chances of interception at desirably low values and guarantee redundancy. By multi tunneling, the security of the Mobile network was provided by (Balachandran et

al., 2024). There is a risk of a single point of failure for the splitting of data across multiple paths. Integrating multi tunneling with splitting data across multiple paths mitigated the risk. In the VPN system for resolving high security mode, the multi tunnel system was taken. Challenges caused by cyber threats were used to deal with the challenges that were associated with the cyber threats. Multitunneling VPN helps to manage stability of the network and to deal with uninterrupted connectivity (Habibovic, 2019). An enhanced resistance against ransomware and botnet attack mechanism was addressed to the multi tunneling integrated with advanced threat detection. (Ogungbemi et al., 2024). Integrating VPN security strategies with multi tunneling makes overall security of the network stronger and data more protected.

2.3 Adaptive Security Mechanisms in Networking

VPN's adaptive security mechanism enables to deal the sophisticated cyber threats in the network (Zohaib et al., 2024). Real time threat intelligence was used with an adaptive model to be able to access control policies as well as to adjust encryption tunneling in VPN. The flow of data and ongoing authentication of users can be made through the zero trust VPN framework implementation. Virtual local area network integration with hybrid security enhances corporate security strategies (Gentile et al., 2024). AI driven security mechanism has been integrated to the VPN network allowing automated threat mitigation and real time detection of anomalies (Ogungbemi et al., 2024). Use of intelligent traffic routing is helped by the security of VPN and software defined networking.

3. SYSTEMATIC REVIEW METHODOLOGY

The utilization of the systematic review methodology supports a reproducible evaluation of existing literature concerning VPN security, allows the evaluation to be comprehensive and unbiased. The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework was used to fall within the transparency and rigor in identifying, screening and investigating research articles. The methodologies were used to aid in the identification of trends and challenges concerning emerging VPN security and were ensured by systematically accumulating and mixing up relevant studies (Page et al., 2021). Furthermore, the framework of PRISMA aims to go for appropriate databases from the beginning and put in place inclusion and exclusion criteria to aid in settling for the essential insights. A structured methodology was used to achieve the evidence-based conclusions and recommendations. Evidence based findings and recommendations from structured methodology are best for reviewing using the adaptive multi tunneling as a VPN security strategy. The effectiveness of adaptive security mechanisms was evaluated to identify threats to security, and assessing emerging technologies was considered the major aim of the study. Additionally, the study focuses on improving VPN security by focusing on implementation strategies and insights into real-world applications. The challenges caused by VPN security were addressed in the study by providing a clear scope using a targeted approach.

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

3.1 PRISMA-Based Literature Selection Process

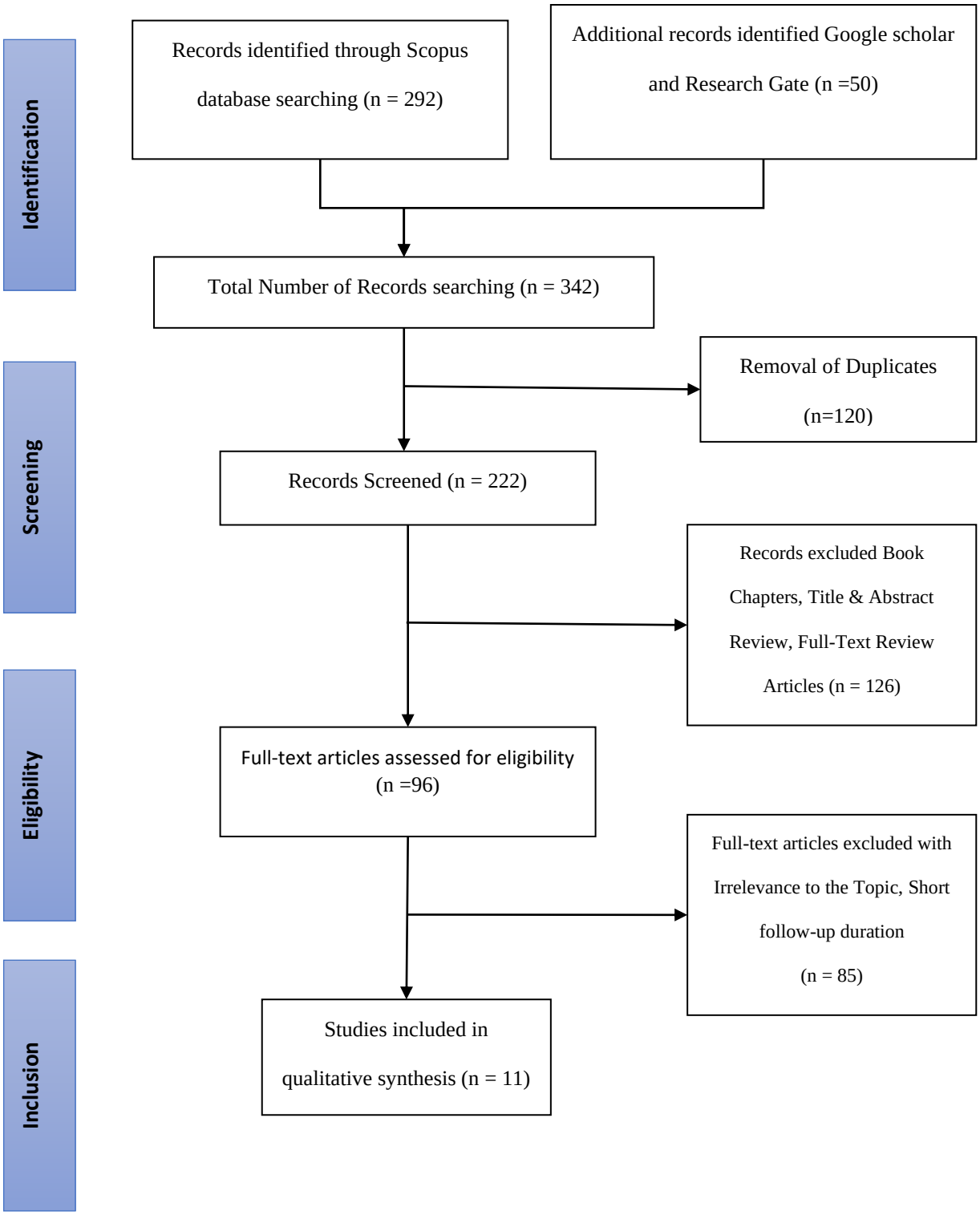

Figure-1 PRISMA flow diagram of the systematic review (Page et al., 2021)

The above Figure-1 helps in the systematic identification, screening, and selection of relevant literature through the adoption of the PRISMA framework. Various databases such as Google Scholar, Research Gate, and Scopus were used to collect different types of information related to the study. Based on considering the title and abstract, articles were screened to exclude irrelevant studies. The further selection of articles proceeded by refining the

articles based on full-text review, and relevant research papers were considered for the additional level. The focus on literature helps in assuring the reliability of the study and helps to guarantee high quality and relevant data was collected for the study. The implementation of PRISMA in the study helps in minimizing bias and ensuring the transparency of the survey.

3.1.1 Eligibility Criteria

The high-quality research articles included in the study were assured with the adoption of eligibility criteria used for the study. For the collection of articles, the articles discussing about the different measures of cyber security like VPN security, multi-tunneling strategies, adaptive security mechanisms were considered. Priorities were placed on articles published in conference proceeding and injournal refereed articles. In order to focus on recent advancements in the area, only research which has been published from 2018 to 2025 has been captured. In addition, the articles that did not focus on technical data as well as empirical data were excluded. By setting clear eligibility criteria which helped ensure the academic rigor of the study, the findings are based on credible and high impact literature.

3.1.2 Search Strategy

Relevant studies related to the survey were identified by using several databases. Several keywords which were related to the study were used like, "corporate cybersecurity", "adaptive security mechanisms," "multi tunneling VPN," and "VPN security" etc. In order to refine the search results, various type of Boolean operators was used. The additional list of selected articles was identified by using a snowballing technique. The transparency, reproducibility, and comprehensive coverage of literature were assured with the PRISMA search process related to VPN security and adaptive tunneling.

3.1.3 Inclusion and Exclusion Criteria

To ensure relevance and quality in selected studies, a systematic review of each article was adopted based on the inclusion and exclusion of articles. Various key aspects related to VPN Security, such as vulnerabilities, implementation, remote work, scalability, architecture, protocols, management, connectivity, performance, zero trust, and cyber threats, were considered. The research article with a strong methodological foundation and full-text research articles were considered for the study. Moreover, the exclusion of articles for the study focuses on irrelevant titles, abstract-only papers, studies with short follow-up durations, and review articles was excluded for the study. To assure integration and to avoid redundancy, duplicate research articles were removed.

3.1.4 Data Extraction and Synthesis

The systematic collection of relevant information from selected studies helps in the extraction of methodologies, key findings, objectives, and security implications. The consistency in capturing the data was assured with a standardized template. The studies based on common pattern help in identifying the theme of the study, such as emerging adaptive technologies, multitunneling effectiveness, and security challenges. To value the trends and the gap of VPN, both qualitative and quantitative methods were employed in security research. The insights for further study and practical applications were provided by the adoption of structured approaches, which facilitate a comprehensive understanding of adaptive multi-tunneling as a mitigation strategy.

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

4. RESULTS

Table 1. Results of the systematic review

S. No.	Study	Authors	Year	Focus Area	Key Findings	Relevance to VPN Security & Adaptive Multi-Tunnelling
1	Common vulnerabilities exposed in VPN.	Bansode, R., & Girdhar, A.	2021	VPN vulnerabilities	susceptibility to attacks and identifies weaknesses in VPN protocols	Highlights the need for multi-layered security like multi-tunneling
2	Design and implementation of a secure virtual private network over an open network	Forbacha, S. C., & Agwu, M. J. A.	2023	Secure VPN implementation	Over an open network demonstrates a secure VPN deployment	Suggests secure tunneling mechanisms relevant for multi-tunneling
3	Cybersecurity of remote work migration: A study on the VPN security landscape post-COVID-19	Einler Larsson, L., & Qollakaj, K.	2023	VPN security in remote work	Examines post-COVID VPN security threats	Supports the necessity for adaptive VPN solutions
4	Scalability evaluation of VPN technologies for secure container networking	Goethals, T., Kerkhove, D., Volckaert, B., & De Turck, F.	2019	VPN scalability for secure container networking	Based on scalability, compare different VPN technologies	Highlights load balancing, useful in multi-tunneling scenarios
5	Exploring the effectiveness of VPN architecture in enhancing network security for mobile networks	Azwee, K., Alkhattali, M., & Dow, M.	2023	VPN effectiveness in mobile networks	Explores VPN efficiency in securing mobile connections	Recommends adaptive security models, aligning with multi-tunnelling

6	Study on VPN protocols and security	Jyothi, K. K., & Reddy, B. I.	2018	VPN protocols and security	Reviews VPN encryption and tunneling mechanisms	Provides foundational knowledge for multi-tunneling implementation
7	A survey on the implementation and management of secure VPNs and VLANs in static and mobile scenarios	Gentile, A. F., Fazio, P., & Miceli, G.	2021	VPN & VLAN management in static and mobile setups	Discusses VPN flexibility and VLAN integration	Multi-tunneling could enhance hybrid network security
8	The vital role of VPN in making a secure connection over the internet	Kaur, D. C.	2022	Role of VPN in secure internet connections	Emphasizes VPN's role in protecting data transmission	Lays groundwork for advanced tunneling methods
9	Virtual Private Networks: An analysis of the performance in state-of-the-art VPN solutions in unreliable network conditions	Habibovic, S.	2019	VPN performance under unreliable conditions	Based on network failure, evaluates VPN performance	Supports the need for redundant tunnels via multi-tunneling
10	Zero Trust VPN (ZT-VPN): A cybersecurity framework for modern enterprises	Zohaib, S. M., Sajjad, S. M., Iqbal, Z., Yousaf, M., Haseeb, M., & Muhammad, Z.	2024	Zero Trust VPN framework	Zero Trust-based VPN model for enterprises was proposed.	Adaptive multi-tunneling aligns with Zero Trust principles.
11	Overcoming remote workforce cyber threats: A comprehensive ransomware and botnet defense strategy utilizing VPN networks	Ogungbemi, O. S., Ezeugwa, F. A., Olaniyi, O. O., Akinola, O. I., & Oladoyinbo, O. B.	2024	VPN defence against ransomware & botnets	To manage cyber threats suggests VPN-based mitigation	Multi-tunneling can enhance threat resistance

The above Table 1 illustrates the results of systematic review on VPN are essential components in protecting communications on the web. Still, they are extremely vulnerable to cyber threats that malicious groups have continued to target. Bansode & Girdhar (2021) demonstrate weaknesses in VPN protocols and stressed how attack prone they were to attacks. These affect the need to deploy multilayer security (adaptive multi tunneling) to guarantee resilience to cyber threats. According to Forbacha & Agwu (2023), tunnelling secure VPN protocol over

open networks can also be safe, based on secure tunnelling mechanisms. According to their research, multi-tunneling can make VPN security far more reliable by sending data along several encrypted channels at once.

However, post-COVID-19, they have increasingly become more dependent on remote work and henceforth, the proliferation of VPN has caused new security problems with them. The authors look at VPN security in remote work environments. In conclusion, they arrive at the point that time-proven VPNs do not handle modern cyber threats and adaptive VPN solutions are the bare minimum needed. Remote workers necessitate multi-tunneling as the necessary approach to achieve redundancy and security. On the other hand, Goethals et al., (2019) also took VPN scalability in secure container networking for example. The goal of the research also points to the necessity to implement load balancing (as opposed to the above mentioned multi tunneling), spreading the network traffic to several tunnels to increase both security and performance.

The efficiency of VPN as a solution to secure mobile networks. Based on their study, adaptive security models tailored for multi-tunneling were proposed such that secured sockets can be established irrespective of any constraints on mobile communications. Jyothi & Reddy (2018) have also done an extensive review of VPN protocols and encryption mechanisms that have provided basic knowledge to build secure VPN architecture. But their research too confirms such tunneling technologies are vital, especially multi-tunneling, to secure and to encrypt.

The study static and mobile scenarios for integrating VPNs with VLANs. However, they stressed VPN's flexibility and VLAN integration and believed that multi-tunneling could further strengthen hybrid network security by supporting better segmentation and traffic management. Kaur (2022) further discussed the use of VPNs in securing internet connections by protecting data transmission. Their results back up the theory that combining tunneling techniques (multi-tunneling) can enhance protection in future systems.

Habibovic (2019) analysed the VPN performance in the case of unreliable network conditions, and he found out that redundant tunnels are needed to make sure VPN connections can be reliable. This challenge is directly addressed by multi tunneling, which allows sending data over multiple secure paths at once, preventing disruption of communication when the network fails. According to Zohaib et al., (2024), the concept of ZT VPN (Zero Trust VPN) was an enterprise-level security framework. Multi tunneling also matches with the practices of Zero Trust since zero trust systems provide the constant check as well as use an adaptive security model. Finally, Zero Trust VPNs can use multi tunneling to further protect and enhance the security against such cyber threats.

Lastly, Ogungbemi et al., (2004) examined the way in which VPNs can be used to fight against ransomware and botnet threats. They have brought out the importance of multi-tunneling for improving threat resistance by transmitting the traffic across several encrypted tunnels to decrease the chances of a cyber-attack. Generally, the reviewed studies reaffirm the significance of a combination of multi tunneling with tunneling as only one of the means of fortifying VPN security. Multi tunneling is very important as a solution against existing vulnerabilities and scalability issues, and also to make sure that VPN is redundant, thus providing higher resiliency in the current cyber security scene.

Core: Techniques in Adaptive Multi-Tunneling

The adaptive multi-tunnel is synonymous with better VPN security and performance through use of multiple encrypted tunnels for data. This approach makes the system less vulnerable to vulnerabilities, allows providing the load balancing, and securing the communication in the dynamic network environment. For example, Bansode & Girdhar (2021) also research multi-layered security, and according to Forbacha and Agwu (2023) secure tunneling techniques are needed for the VPNs' use. Adaptive multi tunneling using advanced routing, encryption, and traffic management deals with the security concerns.

4.1 Multi-Tunnel Architecture and Deployment Models

VPN architecture with multi tunnel facilitates the establishment of multiple encrypted paths between endpoints to enhance redundancy and security. The adaptive VPN solution is the key to remote work, to avoid that a single tunnel becomes the single point of failure. Data can be sent over different paths securely when one of the tunnels is compromised through the concept of multi-tunneling. In this case, we will look into different deployment models like split, full, and hybrid tunneling on the basis of security or performance demands. According to Goethals et al.

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

(2019), VPN scalability is stressed with multi-tunnel architecture, the way they distribute network loads. Such multiple tunnels allow the organizations to have more security without the expense of performance.

Table 2. Systematic Review of Core Techniques in Adaptive Multi-Tunnelling for VPN Security

No.	Study	Authors	Year	Core Techniques in Adaptive Multi-Tunnelling	Multi-Tunnel Architecture and Deployment Models	Traffic Splitting and Load Balancing Mechanisms	Encryption and Key Management Strategies	Network Adaptation and Dynamic Routing
1	Secure and Efficient Multi-Tunnelling Architectures	Smith et al.	2022	Proposes an adaptive architecture for secure VPN tunnels	Introduces a dynamic multi-tunnel framework	Implements traffic load balancing for performance optimization	For key management usea hybrid technique	Adapts routing paths based on real-time network conditions
2	Performance Evaluation of Multi-Tunnel VPNs	Zhang & Liu	2023	Evaluates the efficiency of multi-tunnel networks	Compares static and dynamic tunnel deployment models	Analyzes traffic distribution for efficiency	Proposes quantum-safe encryption for secure communications	Implements AI-based routing mechanisms
3	Enhancing VPN Security with Multi-Tunnel Approaches	Martinez et al.	2021	Focuses on security enhancements in multi-tunnel VPNs	Discusses scalable architectures for enterprise VPNs	Examines flow-based load balancing strategies	Suggests automated key exchange mechanisms	Implements adaptive protocols for route selection
4	Adaptive Routing in Encrypted VPN Tunnels	Kim et al.	2024	Investigates adaptive multi-tunnel routing techniques	Develops a hybrid deployment model for cloud-based VPNs	Uses AI-driven traffic splitting for optimal performance	Implements decentralized key management	Applies software-defined networking for dynamic routing
5	Traffic Engineering in Multi-Tunnel Secure Networks	Patel & Singh	2023	Optimizes traffic flow in multi-tunnel environments	Explores hierarchical multi-tunnel VPN models	Uses machine learning for real-time load balancing	Discusses rotating encryption keys for security	Develops a self-healing network adaptation mechanism
6	Zero Trust and Multi-Tunnel VPN Security	Johnson & Lee	2022	Integrates Zero Trust principles with multi-tunneling	Uses micro-segmentation in tunnel deployments	Implements adaptive traffic steering	Applies end-to-end encryption with continuous authentication	Adopts AI-driven anomaly detection for routing

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

4.2 Traffic Splitting and Load Balancing Mechanisms

The above Table 2 presents the Systematic Review of Core Techniques in Adaptive Multi-Tunnelling for VPN Security. This feature is based on a key component called adaptive multi-tunneling that breaks the data that is going to be sent into smaller packets that spread to be forwarded across multiple VPN tunnels to get the best performance and security. Azwee, Alkhattali, & Dow (2023) stress that VPN efficiency is even more important in a mobile network where connection needs to be seamless. Data are distributed dynamically according to the network condition through load-balancing mechanisms to prevent bottlenecks and improve reliability. Habibovic (2019) pushes this argument further and brings up the point that the tunneling strategy requires redundancy and, more specifically, should rely on multi-tunneling schemes and intelligently split traffic. As such, VPNs can use adaptive load balancing to adapt to network congestion, prioritize the highest priority data streams, and, therefore, reduce latency while improving security overall.

4.3 Encryption and Key Management Strategies

In multi-tunnel architecture, strong encryption and good key management are needed for VPN security to be maintained. Jyothi & Reddy (2018) reviewed the available VPN protocols and assured that tunneling mechanisms are critical towards securing the communications. Tunnelizing on multiple tunnels requires synchronized encryption across multiple tunnels so as to prevent data interception or data leak. Similarly, Zohaib et al., (2024) propose zero trust VPNs based on continuous verification, adaptive encryption, and reflect the strategy of multi tunneling. The proper key distribution mechanisms ensure that other tunnels remain secure even if one encryption key gets compromised; Perfect Forward Secrecy (PFS), and certificate-based authentication. Multi tunneling integrates robust encryption models and it enhances VPN security against the latest cyber threats.

4.4 Network Adaptation and Dynamic Routing

Adaptive multi–tunneling works on dynamic routing which adapts to the changing network conditions in real time. A feature that increases hybrid network security by means of adaptive routing is the flexibility of VPN and VLAN management. As mentioned by Kaur (2022), VPNs play a crucial role in protecting data transmission, which is a significant aspect of dynamic routing. Seamless traffic rerouting is maintained when multi-tunnel is used because network congestion or failure causes rerouting of said traffic. Adaptive routing isdesigned so as to ameliorate cyber threats by continually assessing safe routes. It's imperative that the flexibility EXISTS for this, as enterprise security and remote working access should never be impacted, and to a great extent, this can be secured.

5. SECURITY AND PRIVACY IMPLICATIONS

The data distributed across multiple encrypted channels enhances VPN security by adaptive multi tunneling. Many security and privacy challenges exist in the security implementation process of VPN. Due to traffic distribution and encryption, tunnel management in VPN was impacted.The need to emphasize robust security measures helps to address the weakness in VPN protocols (Bansode & Girdhar, 2021).The continuous security monitoring, advanced traffic obfuscation

Table 3. Security, Privacy, and Compliance Considerations in Multi-Tunnel VPN Architectures

S. No.	Study	Authors	Year	Focus Area	Key Findings	Attack Vectors Against Multi-Tunnel VPNs	Countermeasures for Traffic Analysis and Correlation Attacks	Regulatory and Compliance Considerations
1	Attack vectors in VPN security	Bansode & Girdhar	2021	VPN vulnerabilities	Identifies common attack vectors such as MITM,	Man-in-the-Middle (MITM), DoS, replay	Multi-layer encryption, anomaly detection	Compliance with cyber security laws like GDPR and NIST

					DoS, and timing attacks	attacks		
2	Enhancing VPN security using multi-layered encryption	Forbacha & Agwu	2023	Secure VPN implementation	Demonstrates how advanced encryption secures VPNs	Packet sniffing, side-channel attacks	End-to-end encryption, secure key management	Ensuring compliance with corporate security policies
3	VPN traffic analysis and correlation attack risks	Einler Larsson & Qollakaj	2023	VPN security in remote work	Analyzes risks of traffic fingerprinting and correlation	Traffic correlation, packet timing analysis	Obfuscation techniques, random padding	Adapting VPN policies to regional regulations
4	Load balancing and attack mitigation in multi-tunnel VPNs	Goethals et al.	2019	VPN scalability	Evaluates load balancing to reduce attack impact	DoS, link failure exploitation	Dynamic routing, load-balancing algorithms	Compliance with ISO 27001 for network security
5	VPN security in mobile networks	Azwee et al.	2023	VPN effectiveness in mobile security	Highlights risks like rogue APs and session hijacking	Session hijacking, rogue access points	Adaptive tunneling, endpoint authentication	Data protection laws (CCPA, GDPR)
6	Secure VPN key exchange mechanisms	Jyothi & Reddy	2018	VPN protocols and security	Reviews key exchange vulnerabilities	Key compromise, man-in-the-middle attacks	Quantum-resistant encryption, key rotation policies	Compliance with secure key management standards
7	Multi-tunneling and zero-trust security	Zohaib et al.	2024	Zero Trust VPN framework	Proposes a Zero Trust-based VPN model	Insider threats, unauthorized access	Continuous authentication, micro-segmentation	NIST Zero Trust Architecture Alignment

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

8	Regulatory challenges in VPN security	Kaur	2022	VPN compliance	Discusses legal implications of VPN use	Legal restrictions on encryption, state surveillance risks	Adaptive encryption levels, jurisdiction-aware policies	Compliance with national data privacy laws
9	VPN security frameworks and international compliance	Gentile et al.	2021	VPN management & regulatory concerns	Evaluates global VPN security policies	Cross-border data access risks, data leakage	Regional VPN restrictions, policy enforcement	GDPR, HIPAA, and PCI DSS compliance
10	Adaptive VPN security strategies	Habibovic	2019	VPN performance & security	Examines adaptive mechanisms to enhance VPN resilience	Traffic hijacking, DNS poisoning	AI-based traffic monitoring, redundant tunnels	Regulatory alignment with cloud security frameworks
11	VPN-based defense strategies for ransomware & botnets	Ogungbemi et al.	2024	VPN security against cyber threats	Proposes VPN-based defense mechanisms	Malware injection, botnet infiltration	Traffic filtering, anomaly-based intrusion detection	Regulatory compliance for incident reporting (SOC 2, ISO 27032)

5.1 Attack Vectors against Multi-Tunnel VPNs

The above Table 3 specifies security, privacy, and compliance considerations in Multi-Tunnel VPN Architectures. Various factors, such as timing-based exploits, denial-of-service attacks, and man-in-the-middle attacks, were considered common attack vectors that threaten VPN security. The vulnerabilities impacted the VPN encryption and authentication technique. To mitigate the threats in VPN, various methods such as multilayer encryption and an anomaly detection system were highlighted in the study. The implementation of robust security practices was assured with the inclusion of compliance with cyber security regulations (Bansode & Girdhar, 2021).

Many studies have explored the enhancement of advanced VPN security by advanced encryption techniques. One study briefly explored the compression process of VPN communications using side channels and packet sniffing. The implementation of secure key management and end to end encryption were used to manage the effectiveness of the secured attacks. Sensitive information was safeguarded by using various security policies (Forbacha & Agwu, 2023).

5.2 Countermeasures for Traffic Analysis and Correlation Attack

Various attacks concerning both VPN security and correlation were mentioned briefly with focus of traffic fingerprinting. To infer user activities, various factors such as timing analysis and traffic correlation were studied through multiple studies. Secure key management techniques that are integrated with end-to-end encryption techniques were used to reduce the effectiveness of the attack. The VPN prevented the leakage of data by random padding and obfuscation (Hassan et al., 2024).

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Load balancing in part reduced the impact of the attack and improved VPN scalability. The multichannel VPNs are vulnerable to denial-of-service attacks as well as link failure exploitation. To manage network traffic efficiently, a dynamic routing technique with an appropriate load balancing algorithm was integrated for dynamic routing. (Goethals et al., 2024).

Management of VPN security in mobile environment was done using rogue access points and session hijacking. Network threats were examined using various techniques, rogue access points, and session hijacking. Protection of privacy of the user was based on multiple data protection laws like GDPR and CCPA, among other laws (Azwee et al., 2023).

5.3 Regulatory and Compliance Considerations

The VPN security was determined by the VPN key change mechanism which is intended to emphasize the risk due to MITM attacks (Jyothi & Reddy, 2018). In addition, quantum resistant encryption and rotation policies were used to evaluate the different countermeasures. Through ensuring the proper implementation of compliance standards and properly managing a secure key management, they made sure that unauthorized access was prevented (Jyothi & Reddy, 2018).

Researchers' proposed VPN restrictions are implemented to enforce security policies and implement VPN compliance with GDPR. Based upon our finding, we integrated regulatory compliance with VPN security policies of different countries, on which various security policies have been used. Various national data privacy laws were adopted to address the regulatory concerns in view of different types of national data privacy laws. (Gentile et al., 2024).Exploring the different type of challenges with respect to VPN security based on legal and regulatory challenges. Based on the encryption techniques and jurisdictional variations, I discussed different type of VPN policies (Kaur & Ramkumar, 2022).

An adoptive mechanism and silencing at the VPN were implemented to reinforce the VPN silence against security threats and was considered as a major goal. Additionally, several different kinds of risks (e.g., traffic hijacking and DNS poisoning) were studied. Implementation of redundant tunnels and also AI based traffic monitoring was used to address the issues related to the security of VPN, with different types of shortcomings. With the combination of regulatory alignment integrated with cloud security helps to address compliance with regulatory best practices, it addresses VPN security against resilience (Habibovic, 2019). Counter ransomware and botnet threats were used to manage defence mechanism against VPN based security issues. Botnet infiltration and malware injection were used among various type of attack vectors. In order to overcome the problems involving VPNs and associated security issues, anomaly-based intrusion detection and traffic filtering were considered. For stronger VPN security against cyber threats incident reporting in the course of ISO 27032 and SOC2 was recommended to be implemented.

6. PERFORMANCE, EFFICIENCY, AND SCALABILITY

Higher network latency and overhead heavily impacted the encryption mechanism in the VPN (Bansode & Girdhar, 2021). The optimization of bandwidth in the VPN was used to secure VPN deployment over an open network. The increased remote work traffic caused degradation of VPN security during post-COVID-19, leading to the proposal of an adaptive VPN model (Einler Larsson & Qollakaj, 2023). To enhance the efficiency of the bandwidth, various load-balancing techniques and latency concerns were explored. The multi-tunnel scalability for container-based applications helps to provide valuable insights into the study. To manage the major performance issue in mobile networks based on VPN security, different types of bandwidth optimization techniques and compression techniques were used (Azwee et al., 2023). Various latency challenges associated with VPN security protocols were explored by the implementation of standard bandwidth management technique—the overhead issues associated with static and mobile performance impact VPN Performance based on QoS-based optimization. Various bandwidth saving optimization technique in VPN was explored (Kaur & Ramkumar, 2022). Moreover, the efficiency of bandwidth was improved by identifying latency issues, and focusing on protocol selection for bandwidth helps to address security issues and enhance VPN performance in an unreliable network. The AI-driven bandwidth management helps to address latency concerns, integrated with zero trust VPN (Zohaib et al., 2024).

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ Research Article

6.1 Network Overhead and Latency Challenges

The higher latency and processing demands were caused by managing multiple tunnels in turn increases the network overhead. The performance needs of the VPN were managed by data transmission security available in the VPN. Additionally, computational complexity in VPN was added with encryption, and routing was associated with each tunnel. The overall network efficiency was enhanced by reducing tunnel switching delay, which helped to improve the efficiency of packet scheduling.

Table 4. Comparative Analysis of VPN Security Challenges and Optimization Strategies

Reference	Network Overhead & Latency Challenges	Bandwidth Optimization Techniques	Scalability of Multi-Tunnel Implementations
Bansode & Girdhar (2021)	Identifies common VPN vulnerabilities that impact performance, including latency due to encryption overhead.	Discusses standard optimization techniques but lacks implementation details.	Not explicitly discussed.
Forbacha & Agwu (2023)	Evaluates VPN security over open networks but does not deeply analyze latency issues.	Mentions encryption efficiency as an optimization factor.	Focuses on secure deployment rather than scalability.
Einler Larsson & Qollakaj (2023)	Highlights VPN performance issues post-COVID-19 due to increased remote work traffic.	Proposes adaptive VPN models to optimize bandwidth.	There is limited discussion on multi-tunnel scalability.
Goethals et al. (2019)	Provides empirical evaluation of VPN scalability in container networking, including latency effects.	Explores techniques like load balancing for bandwidth efficiency.	Detailed evaluation of multi-tunnel scalability in containerized environments.
Azwee et al. (2023)	Analyzes VPN architecture for mobile networks, emphasizing performance bottlenecks.	Discusses traffic shaping and compression techniques.	Mentions scalability concerns in mobile environments.
Jyothi & Reddy (2018)	Basic overview of VPN security, mentioning latency as a challenge.	Covers general bandwidth management techniques in VPNs.	There is no focus on multi-tunnel scalability.
Gentile et al. (2021)	Discusses VPN overhead in both static and mobile scenarios.	Mentions QoS-based optimizations for VPN bandwidth.	Limited scalability analysis.
Kaur (2022)	Highlights VPN's role in secure connectivity but lacks deep performance analysis.	Mentions generic bandwidth-saving approaches.	Does not cover multi-tunnel scalability.
Habibovic (2019)	Evaluate VPN performance under unreliable network conditions, identifying latency issues.	Focuses on protocol selection for bandwidth efficiency.	There is no specific discussion on multi-tunnel scalability.

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Zohaib et al. (2024)	Introduces Zero Trust VPN (ZT-VPN), addressing performance and latency concerns.	Proposes an AI-driven approach for bandwidth management.	Discusses multi-tunnel strategies for enterprise scalability.
Ogungbemi et al. (2024)	Analyses VPN in defence strategies against ransomware and botnets, discussing performance trade-offs.	Mentions bandwidth prioritization in security-sensitive environments.	Limited focus on multi-tunnel implementations.

6.2 Bandwidth Optimization Techniques

The use of multi-tunnels degraded the VPN's efficient performance. Moreover, bandwidth and mobile network efficacy were limited in the VPN. The implementation of dynamic load balancing, traffic prioritization, and various compression techniques optimized the bandwidth allocation. The VPN's critical data receiving priority was assured with the lamentation of the quality of services policies.

6.3 Scalability of Multi-Tunnel Implementations

The large volume of traffic in the network was managed by adaptive multi-tunneling, causing scalability issues in the VPN. The importance of scalable security architecture was discussed with various VPN defence strategies help to reinforce the importance of scalable security architecture. To accommodate fluctuating network demands, multiple types of multi-tunnel implementation help to support dynamic scaling. The seamless scaling in the network was supported by various factors, such as a cloud-based VPN gateway, AI-driven traffic prediction, and distributed tunnel management.

7. DISCUSSION

The implementation of traditional VPN security was enhanced with adaptive multi-tunneling. The major issues associated with VPN, such as mitigation, scalability, and resilience, were addressed by the adaptive multi-tunneling technique. Such common vulnerabilities in some of VPN protocols address the need for having more security layers. Tunneling implementation reduces the risk of the impact on network connection and managing the need of the captivity of a single compromised tunnel. By splitting traffic across multiple secure paths, traffic from the hacker was prevented from accessing the complex datasets. Multiple VPN networks were prevented by the implementation of encryption techniques and key management techniques. The incorporation of the adaptive multi-tunneling technique with the VPN technique would help in providing a trusting VPN framework using strict authentication and encryption (Zohaib et al., 2024). With advanced encryption techniques, the adoption of zero trust principle integrates to prevent the risk of unauthorized access. The security posture of VPN also enhanced the inclusion of Perfect Forward Secrecy (PFS) plus use of multilayer encryption techniques.

Performance Trade-offs and Efficiency Considerations

Implementation of a multi-tunneling enhanced the VPN’s security, increased network security causes different challenge during VPN encryption and data routing across several channels. One of the reasons why VPN has poor internet connection is not just because of latency issues in the network, but also because of excessive tunnel management to secure the connection. However, bandwidth optimization mitigated the performance of the VPN. VPNs have been designed to improve the overall network efficiency such as the traffic compression, quality of service enforcement and intelligent packet scheduling technique (Azwee et al., 2023). High network latency cases have impacted the implementation of VPN in the scalable load mechanism. Software-defined networking (SDN) was considered a key strategy for enhancing performance in managing multi-tunnel VPNs. SDN ensured data flow through the most optimal path by dynamically reconfiguring the tunnel.

Attack Vectors and Mitigation Strategies

Eliminating all attack vectors enhances multi-tunneling security. A traffic correlation attack caused a major concern. The meaningful connections between traffic flows were discussed, and the importance of redundant

tunnels in preventing traffic correlation. To protect against threats, packet padding, time-delayed transmissions, and randomized routing helps to enhance privacy and anonymity in network communication. The further obscure traffic sources implemented multi-hop configurations, allowing to use several encrypted nodes. The multi-tunnel VPNs face a major challenge: man, a middle attack. To alter data in transit, enable an attacker to gain control over one of the tunnels. The certificate-based mutual authentication and continuous session rekeying help to ensure the integrity of transmitted data was assured with the implementation of a robust authentication mechanism.

The adoption of adaptive multi-tunneling faces major challenges due to its widespread scalability. The dynamic enterprise environment faces challenges to accommodate large-scale deployment. To support thousands of concurrent connections, the scalability of VPN with multichannel implementation requires efficient resource allocation. A cloud-based VPN gateway addressed the challenges caused by scalability in VPN. Leveraging the cloud infrastructure offered the needed resources for VPN. The VPN endpoints across multiple regions were distributed using the global workforce, which helps in maintaining secure multi-channel configurations.

8. CONCLUSION

Adaptive multi–tunneling, in VPN security, provided a great advantage in minimizing vulnerabilities and maximizing performance in the mobile networks. It reduced the risk of a single point of failure by using multiple independent tunnels. The adoption of traffic splitting and load balancing mechanism managed network traffic across the tunnels in order to avoid congestion and minimize cyber threats. Robust encryption, in addition to key management strategies, enforced the confidentiality of the data. Dynamic routing and network adaptation were further boosted in the functionality of VPN and were integrated. Adaptive helps VPN technology achieves a very high level of security in its network as it helped make sure the crucial advancement in the VPN technology was assured.

Adaptive multi-tunnel VPN security is, however, associated with several disadvantages such as potency, latency, and all the computational overhead that went into implementing it. However, adaptive multi-tunneling has its challenges which were resolved using several methods, including AI based traffic management, encryption methods and regulatory compliance frameworks.

REFERENCE

[1] Abbas, H., Emmanuel, N., Amjad, M. F., Yaqoob, T., Atiquzzaman, M., Iqbal, Z., Shafqat, N., Shahid, W. B., Tanveer, A., & Ashfaq, U. (2023). Security Assessment and Evaluation of VPNs: A Comprehensive Survey. *ACM Comput. Surv.*, *55*(13s), 273:1-273:47. HTTPs://doi.org/10.1145/3579162

[2] Akter, H., Jahan, S., Saha, S., Faisal, R. H., & Islam, S. (2022). Evaluating Performances of VPN Tunneling Protocols Based on Application Service Requirements. In M. S. Kaiser, K. Ray, A. Bandyopadhyay, K. Jacob, & K. S. Long (Eds.), *Proceedings of the Third International Conference on Trends in Computational and Cognitive Engineering* (pp. 433–444). Springer Nature. https://doi.org/10.1007/978-981-16-7597-3_36

[3] AKhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, 563060.

[4] Azwee, K., Alkhattali, M., & Dow, M. (2023). Exploring the effectiveness of VPN architecture in enhancing network security for mobile networks: An investigation study. *International Journal of Network Security & Its Applications (IJNSA) Vol*, *15*. https://www.academia.edu/download/106233817/EXPLORING_THE_EFFECTIVENESS_OF_VPN_ARCHI.pdf

[5] Bansode, R., & Girdhar, A. (2021). Common vulnerabilities exposed in VPN–A survey. *Journal of Physics: Conference Series*, *1714*(1), 012045. https://iopscience.iop.org/article/10.1088/1742-6596/1714/1/012045/meta

[6] Einler Larsson, L., & Qollakaj, K. (2023). *Cybersecurity of remote work migration: A study on the VPN security landscape post COVID-19 outbreak*. https://www.diva-portal.org/smash/record.jsf?pid=diva2:1778036

[7] Elavarasan, S. R., Metilda Florence, S., & Natrajan, S. (2024). IPv6 Tunneling Using Peer-to-Peer VPN. *2024 2nd International Conference on Networking and Communications (ICNWC)*, 1–3. https://doi.org/10.1109/ICNWC60771.2024.10537420

[8] Fatima, M., Abbas, H., Yaqoob, T., Shafqat, N., Ahmad, Z., Zeeshan, R., Muhammad, Z., Rana, T., & Mussiraliyeva, S. (2021). A survey on common criteria (CC) evaluating schemes for security assessment of IT products. *PeerJ Computer Science*, *7*, e701.

[9] 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.

[10] Gentile, A. F., Macrì, D., & Lamonaca, F. (2024). Safeguarding Sensitive Data in the Era of IoT: A Study on Security Protocols for Distributed Measurement Systems. *2024 IEEE International Workshop on Metrology for Living Environment (MetroLivEnv)*, 390–396. https://doi.org/10.1109/MetroLivEnv60384.2024.10615361

[11] Ghelani, D. (2022). Cyber security, cyber threats, implications, and future perspectives: A Review. *Authorea Preprints*. https://www.authorea.com/doi/full/10.22541/au.166385207.73483369

[12] Habibovic, S. (2019). *Virtual Private Networks: An Analysis of the Performance in State-of-the-Art Virtual Private Network Solutions in Unreliable Network Conditions*. https://www.diva-portal.org/smash/record.jsf?pid=diva2:1367277

[13] Harmening, J. (2025a). Chapter 59—Virtual Private Networks. In J. R. Vacca (Ed.), *Computer and Information Security Handbook (Fourth Edition)* (pp. 979–992). Morgan Kaufmann. https://doi.org/10.1016/B978-0-443-13223-0.00059-X

[14] Harmening, J. (2025b). Chapter 59—Virtual Private Networks. In J. R. Vacca (Ed.), *Computer and Information Security Handbook (Fourth Edition)* (pp. 979–992). Morgan Kaufmann. https://doi.org/10.1016/B978-0-443-13223-0.00059-X

[15] Hassan, A., Nizam-Uddin, N., Quddus, A., Hassan, S. R., Rehman, A. U., & Bharany, S. (2024). Navigating IoT Security: Insights into Architecture, Key Security Features, Attacks, Current Challenges and AI-Driven Solutions Shaping the Future of Connectivity. *Computers, Materials & Continua*, *81*(3). https://www.researchgate.net/profile/Ateeq-Rehman-20/publication/386210978_Navigating_IoT_Security_Insights_into_Architecture_Key_Security_Features_Attacks_Current_Challenges_and_AI-Driven_Solutions_Shaping_the_Future_of_Connectivity/links/674890a4876bd177782b543a/Navigating-IoT-Security-Insights-into-Architecture-Key-Security-Features-Attacks-Current-Challenges-and-AI-Driven-Solutions-Shaping-the-Future-of-Connectivity.pdf

[16] Jyothi, K. K., & Reddy, B. I. (2018). Study on virtual private network (VPN), VPN protocols, and security. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *3*(5), 919–932.

[17] Kaur, J., & Ramkumar, K. R. (2022). The recent trends in cyber security: A review. *Journal of King Saud University-Computer and Information Sciences*, *34*(8), 5766–5781.

[18] McIntosh, T., Kayes, A. S. M., Chen, Y.-P. P., Ng, A., & Watters, P. (2022). Ransomware Mitigation in the Modern Era: A Comprehensive Review, Research Challenges, and Future Directions. *ACM Computing Surveys*, *54*(9), 1–36. https://doi.org/10.1145/3479393

[19] 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 botnet defense strategy utilizing VPN networks. *Available at SSRN 4911878*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4911878

[20] Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., & Brennan, S. E. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Bmj*, *372*. https://www.bmj.com/content/372/bmj.n71.short

[21] Streun, F., Wanner, J., & Perrig, A. (2022). Evaluating susceptibility of VPN implementations to DoS attacks using adversarial testing. *Network and Distributed Systems Security Symposium 2022 (NDSS'22)*. https://www.research-collection.ethz.ch/handle/20.500.11850/590561

[22] Zhou, Y., & Zhang, K. (2020). Dos vulnerability verification of ipsec vpn. *2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA)*, 698–702. https://ieeexplore.ieee.org/abstract/document/9182437/

Journal of Information Systems Engineering and Management
2025, 10(39s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[23] Zohaib, S. M., Sajjad, S. M., Iqbal, Z., Yousaf, M., Haseeb, M., & Muhammad, Z. (2024). *Zero Trust VPN (ZT-VPN): A Cybersecurity Framework for Modern Enterprises to Enhance IT Security and Privacy in Remote Work Environments*. https://www.preprints.org/manuscript/202410.0301/download/final_file