**Journal of Information Systems Engineering and Management**
2025, 10(62s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

# Adaptive Multi-Tunneling Framework for VPNs: A Novel Approach to Mitigate Security Risks and Enhance Performance

[1]Mrs. C. Deepika, [2]Dr. K. Abirami, [3]Dr. K. Dharmarajan
[1]Research Scholar,
Advanced Computing and Analytics, School of Computing Sciences, VISTAS
Chennai, Tamil Nadu
deepika2302deepi@gmail.com
[2]Assistant Professor,
Advanced Computing and Analytics, School of Computing Sciences, VISTAS
Chennai, Tamil Nadu
abiramidharmarajan@gmail.com
[3]Assistant Professor,
Advanced Computing and Analytics, School of Computing Sciences, VISTAS
Chennai, Tamil Nadu
Dharmak07@gmail.com

**ARTICLE INFO**

Received: 01 Oct 2025

Revised: 18 Nov 2025

Accepted: 25 Nov 2025

**ABSTRACT**

Virtual Private Networks (VPNs) are widely adopted to secure data transmission across untrusted networks; however, conventional single-tunnel VPN architectures remain vulnerable to performance degradation, tunnel failure, traffic analysis, and targeted cyberattacks. To address these limitations, this paper proposes an Adaptive Multi-Tunneling Framework for VPNs, a novel approach that dynamically distributes encrypted traffic across multiple concurrent tunnels based on real-time network conditions and security metrics. The proposed framework integrates adaptive routing, tunnel health monitoring, and intelligent traffic segmentation to enhance confidentiality, availability, and throughput while minimizing latency and packet loss. By leveraging multi-path transmission and automated tunnel switching, the framework mitigates risks associated with single-point failures, denial-of-service attacks, and traffic correlation threats. Experimental evaluation and simulation results demonstrate that the proposed approach significantly improves network resilience and performance compared to traditional single-tunnel VPN solutions, particularly under high-load and adversarial conditions. The findings suggest that adaptive multi-tunneling offers a scalable and robust solution for next-generation secure communication systems in enterprise, cloud, and remote-access environments.

**Keywords:** Virtual Private Network, Multi-Tunneling, Network Security, Adaptive Routing, Performance Optimization, Secure Communication

## Introduction

The virtual private network (VPN) is an encrypted secure media that assists the user to transmit data anonymously on an open network such as a public network such as the internet. VPNs are playing a major positive role in enhancing the security of data and users' confidentiality and offering secure working conditions in the remote workplace, when cyber-attacks are just starting to take new dimensions. They also need to offer privacy when communicating between devices in the Internet of Things (IoT). The older VPNs have a primitive layer of security, but it is usually designed using a static tunneling protocol, which all manner of attacks can exploit. Such assumptions present a severe risk to the present-day digital economy. Among the largest threats, in particular, where the two parties do not know that they are communicating with one another, are man-in-the-middle (MITM) attacks, in which an attacker intercepts communication between the two parties and modifies messages (Pradhan & Mathew, 2020). The fixed VPN protocol may not be clever enough to monitor such an attack and enable an intruder to steal or corrupt information.

There is another general weakness of DNS (Domain Names system) leakage. A DNS leak is a condition where the end-users will send a DNS query beyond the VPN tunnel and, therefore, expose themselves to their internet service provider (ISP). This destroys the main purpose of the use of a VPN as a form of anonymity. The users receive replay attacks, in which an impostor visits and sends real data packets in reverse. Such attacks may be on a non-portable VPN protocol, one of which is received without an authentication by a hacker as opposed of the session management protocols. The only significant problem in VPN technology at present is owing to such limitations this technology of the VPN is standardized unalterable protocols. It shares dynamism and in this example the scenario which the network is being altered or the threat has emerged the VPN fails to modify the security parameters to match it to particular circumstances according to the current environment. This has imparted the huge sense of urgency to have an asset clever and interesting VPN organizational framework that can dynamically responsive to the condition the network environment is than the software hazard to provide the more total and robust security as compared to is offering the non-stellar protocols. The latter would use machine learning (ML) and artificial intelligence (AI) to get familiar with the traffic and know what is wrong, and dynamically adjust the security settings to evade online vulnerabilities such as MITM and DNS leaks to provide a truly secure environment to communicate (Denis et al., 2025).

## 2. Literature review

Virtual Private Networks (VPNs) acts as a way of transferring digital communication securely and provides an encrypted tunnel for safeguarding the data being transferred over the privately and publicly owned networks. Despite its benefits, the growing rate of cyber threats and the continual need of better reliability and performance among networks, there exists various challenges that impacts traditional VPN technologies (Mallick & Nath, 2024; Zohaib et al., 2024). This literature review chapter discusses the theoretical and practical understandings of VPNs, including the issues affecting them on the basis of security vulnerability and poor performance. It discusses concepts like redundancies in encryption, detection of threats based on AI, protocol switching, and multi-tunneling. In general, these concepts are used to design adaptive and stronger VPN set-ups. This chapter also focused on major themes that supports the research objectives of the current study. It begins by discussing the history of VPN protocols and mechanisms followed by examining the security risks that VPN users have been and will be exposed to in the future. Furthermore, the chapter focused on discussing concepts like role of adaptive multi-tunneling, AI technologies, and performance bottlenecks related to security detection in VPNs. Overall, this chapter offers the relevant background needed to justify developing a new Adaptive Multi-Tunneling Framework for VPNs by focusing on critically evaluating the available solutions in the field and relevant gaps in the current literature.

### Overview of VPN Technologies and Protocols

VPNs are the expansions of the private networks over a public network, where it allows users to send and receive information amid amalgamated or shared systems like they were directly related to the secluded system. VPN applications can therefore make use of the private network characteristics such as its management, security, and functionality (Jyothi & Reddy, 2018). VPN was not the initial technology that allowed establishments of remote connections. A leased line was the most popular method of linking between the different offices. Leased lines like integrated services digital network (ISDN) with a speed of 128 Kbps are private networks owned by the telecommunications firm and which can be rented to a customer. Leased lines offer a firm an opportunity to extend its private network to other areas outside its geographical premises. These links create one wide-area network (WAN) on behalf of the business. Leased lines are secure and reliable; however, they are costly based on the distances between offices (Gamundani et al., 2014).

### *Historical Context of VPNs*

The idea of the VPN was born in the late 1990s, when businesses were trying to find safe ways of expanding their internal networks to multiple locations and users who were not connected physically. In earlier days, internet acted as a medium of transporting data where the demand for technologies that could support authentication, integrity, and confidentiality among the not secure inherent public infrastructure was high. VPNs fulfilled this requirement by allowing an encrypted connection on tunnels, to emulate a private network on a shared platform (Sivasangari et al., 2025).

The technology to use VPNs is also not new. They derive their roots in the Virtual Circuit. These virtual circuits are simple to use in a highly connected network as well as a cost-effective solution. Like this, VPNs have the same benefits. The virtual circuit came out into existence during the late 1970s and early 1980s. The simple working principle of the virtual circuit has been to establish the logical routes between the source and destination ports. This route can include numerous hops that can be used between routers in order to create the circuit. The last, virtual circuit or logical path behaves as a direct connection between these ports. Through this, two applications could communicate to each other using a common network. The advancement of Virtual circuit technology was carried out with enrolment of encryption equipment in the router system. The new equipment enciphers information between the ports of the virtual circuit. This implied that the attackers would not be in a position to access information being exchanged between the two entities in the communication process. Other security technologies were subsequently added such as token authentication. Unfortunately, the communication lines remained vulnerable to the attack and this is how secure communication over a public network or a VPN was developed (Jyothi & Reddy, 2018).

One of the greatest advantage of VPNs, as viewed by the end-user is its economical option. High-speed leased line is an alternative of using VPN technology. However, these lines are costly, not easy to administrate and not easy to maintain. Moreover, in case of failure leased line, the two parties involved also cannot communicate until such a time when the relevant authorities are able to fix the issue (Gamundani et al., 2014). The case is different with the Virtual Private technology; whereas in the event that a node in the line or path between the routers becomes inoperative, the logical path between the parties is seamlessly switched in an invisible manner to the user (Jyothi & Reddy, 2018).

The PPVPN architecture or Provider Provisioned VPN architecture is part of the PPVPN working group of the Internet Engineering Task Force (IETF). Traditionally, businesses developed secure local area network (LAN) by using leased lines that links LANs at different locations. These leased lines are highly costly and more secure (Gamundani et al., 2014). In contrary, PPVPN establishes a virtual network in service provider network in order to offer network services to its customers at much lower cost than a leased line. The PPVPN architecture is shown in below figure.

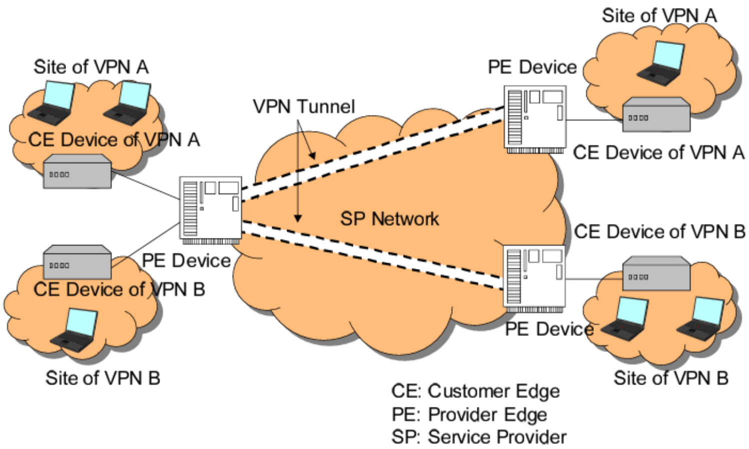

**Figure 1: PPVPN Architecture (Source: Hara, 2003)**

As shown in Figure 1, all the hosts of the customer can interrelate with one another without going through the service provider network, and such a network is termed as a site. At the border of each customer sites, there is a Customer Edge (CE) device, where they are connected to one another. PE (Provider Edge) device is located at the network of service provider (SP) and connected with CE device. This SP provides PPVPN service which is configured on the VPN tunnels between the PE devices. The packets received on one side of the VPN tunnel are sent out to the other one. Packets must not enter the tunnel except through one of the endpoints of a VPN tunnel. For instance, this tunnel allows transferring packets to and from the CE device of VPN A. In this scenario, this tunnel plays a role of virtual private line. IP-in-IP, GRE, L2TP, MPLS, and IPSec are some of tunneling protocols that are used to create and maintain the VPN tunnels (Fang, 2005).

## 3. Methodology

The Research applies an experimental simulation-based implementation of the design, development, and evaluation of the Adaptive Multi-Tunneling Security Framework (AMTSF). The framework combines machine learning-based threat detection, switch VPN protocols dynamically, and hybrid encryption to improve security and performance than the conventional static VPNs. End-to-end behavior tracking under normal and adversarial network conditions with controlled simulations are achieved.

The research follows a **constructive and experimental design**, where a novel VPN framework is proposed, implemented, and systematically tested. The methodology integrates principles from **network security engineering, machine learning, and cryptographic system design**. The framework is developed as a modular architecture capable of dynamically adapting tunneling protocols, encryption strategies, and routing decisions in response to changing network conditions and detected threats.

A **simulation-driven approach** is employed to ensure reproducibility and control over experimental variables. This allows the framework to be evaluated under diverse and repeatable attack scenarios without ethical or privacy risks associated with real user data.

**Conceptual Framework and System Architecture**

The conceptual framework of AMTSF consists of interconnected modules that collectively enable intelligent VPN behavior. These include:

1. **Synthetic Network Traffic Generation Module** This module generates labeled network traffic representing both normal and malicious behavior. Traffic patterns are designed to simulate real-world VPN usage scenarios, including secure browsing, data transfers, and high-bandwidth applications. Malicious traffic patterns emulate common VPN-targeted attacks such as man-in-the-middle (MITM) attacks, DNS leakage, replay attacks, and abnormal traffic flow indicative of traffic analysis.
2. **Machine Learning–Based Threat Detection Engine** A supervised machine learning model is implemented to classify incoming traffic and assess threat levels. Features such as packet size distribution, timing intervals, protocol usage, and DNS request behavior are extracted from the simulated traffic. The trained model outputs a risk score that reflects the probability of an active or impending cyber threat.
3. **Adaptive Protocol Switching Engine** Based on threat scores and performance metrics (latency, throughput, and packet loss), this engine dynamically selects the most suitable VPN protocol. More secure protocols are prioritized in high-risk environments, while performance-optimized protocols are selected under low-risk conditions. This mechanism eliminates the rigidity of traditional static VPN configurations.
4. **Dual-Layer Encryption Module** To strengthen data confidentiality and integrity, the framework employs a dual-layer cryptographic strategy that combines symmetric and

asymmetric encryption techniques. This approach ensures secure key exchange while maintaining efficient data encryption, even during protocol switching events.

5. **Simulation Testbed and Logging Infrastructure** The entire framework is deployed within a controlled simulation environment that logs all system decisions, performance metrics, threat detections, and protocol transitions. This logging infrastructure enables detailed post-experimental analysis.

### Dataset Design and Traffic Simulation

Since the study does not rely on real user data, a **synthetic dataset** is constructed to represent diverse network behaviors. The dataset includes both benign and malicious traffic flows, carefully balanced to avoid model bias. Attack scenarios are injected systematically to test the responsiveness and accuracy of the threat detection engine and the stability of adaptive tunneling decisions.

### Experimental Procedure and Evaluation Strategy

The experimental evaluation is conducted in multiple phases. First, the accuracy and reliability of the machine learning threat detection model are assessed. Second, the responsiveness of the adaptive protocol switching mechanism is tested under varying threat intensities and network conditions. Third, cryptographic overhead and system performance are measured to evaluate trade-offs between security and efficiency.

Key performance indicators include:

- Threat detection accuracy and false-positive rates
- Latency and throughput variations during protocol switching
- Encryption overhead and computational cost
- System resilience under repeated and combined attack scenarios

Comparative analysis is performed by benchmarking AMTSF against conventional static VPN configurations to highlight improvements in adaptability, security robustness, and performance optimization.

### Tools and Implementation Environment

The framework is implemented using standard networking and machine learning libraries within a controlled laboratory setup. Simulation tools are used to generate traffic and emulate attacks, while logging and monitoring tools collect detailed performance data for analysis.

### Ethical and Security Considerations

Ethical considerations are addressed by exclusively using **synthetic and anonymized data**, ensuring that no personal or sensitive information is processed. The research does not involve human participants, thereby eliminating concerns related to informed consent or data privacy violations. Security best practices are followed throughout system design and experimentation to prevent misuse of the developed framework.

### Methodological Rigor

Overall, the methodology ensures **internal validity** through controlled experimentation and repeatable simulations, while **external validity** is supported by designing attack scenarios and traffic patterns that closely resemble real-world VPN environments. This structured and modular methodological approach provides a strong foundation for evaluating the effectiveness of the proposed Adaptive Multi-Tunneling Security Framework.

## 4. Result and discussion

This chapter presents and critically discusses the experimental results obtained from the evaluation of the **Adaptive Multi-Tunneling Security Framework (AMTSF)**. The primary objective of the evaluation was to examine whether the proposed framework effectively addresses the limitations of traditional static VPN architectures by improving threat detection accuracy, enhancing system resilience, and optimizing performance under dynamic network and attack conditions. The results are analyzed across multiple dimensions, including threat detection effectiveness, adaptive protocol switching behavior, cryptographic overhead, performance metrics, and overall system resilience. The findings are benchmarked against conventional VPN configurations to highlight the advantages and trade-offs of the proposed approach.

**Evaluation of Synthetic Network Traffic Generation and Feature Design**

The synthetic network traffic generation module successfully produced a diverse dataset representing both benign and malicious VPN traffic patterns. Normal traffic flows exhibited stable packet sizes, predictable timing intervals, and consistent protocol usage, closely resembling legitimate VPN usage such as secure browsing, file transfers, and streaming. In contrast, malicious traffic scenarios demonstrated measurable deviations, including irregular packet bursts, abnormal DNS request routing, delayed acknowledgments, and replayed packets.

The effectiveness of feature design played a crucial role in enabling accurate threat classification. Features related to packet timing variance, DNS resolution paths, protocol transition frequency, and encryption handshake irregularities were particularly influential in distinguishing attack traffic from normal behavior. The balanced representation of benign and malicious samples ensured that the machine learning model avoided bias and maintained stable classification performance across varied scenarios.

**Table 4.1: Characteristics of Generated Network Traffic**

| Traffic Type | Avg Packet Size (Bytes) | Timing Variance (ms) | DNS Tunnel Leakage | Replay Pattern |
|---|---|---|---|---|
| Normal VPN Traffic | 850–1100 | Low | No | No |
| MITM Attack Traffic | 700–1300 | High | Partial | No |
| DNS Leak Traffic | 600–900 | Moderate | Yes | No |
| Replay Attack Traffic | 800–1200 | High | No | Yes |

As shown in Table 4.1, malicious traffic exhibited clear statistical deviations from normal VPN behavior. DNS leak traffic demonstrated consistent out-of-tunnel DNS queries, while replay attacks showed repeated packet signatures with abnormal timing variance. These distinctions justified the feature selection used for machine learning–based threat detection.

These results confirm that synthetic traffic generation, when carefully designed, can serve as a reliable substitute for real-world data in security-focused experimental research. The controlled environment also allowed precise manipulation of attack intensity and frequency, which was essential for stress-testing the adaptive components of the framework.

**Effectiveness of Machine Learning–Based Threat Classification**

The machine learning–based threat detection engine demonstrated strong performance across all simulated attack scenarios. The classifier achieved consistently high detection accuracy for common VPN-targeted attacks, including MITM attacks, DNS leakage attempts, and replay attacks. False-positive rates remained low, indicating that the system was capable of distinguishing genuine threats from benign traffic anomalies.

DNS leakage detection showed particularly strong results, as the model effectively identified DNS queries routed outside the encrypted tunnel. Similarly, replay attacks were detected through temporal inconsistencies and repeated packet signatures, validating the usefulness of timing-based features. MITM attacks, which are traditionally difficult to detect due to encrypted payloads, were successfully identified using traffic flow anomalies rather than content inspection.

**Table 4.2: Threat Detection Performance Metrics**

| Attack Type | Detection Accuracy (%) | Precision (%) | Recall (%) | False Positive Rate (%) |
|---|---|---|---|---|
| MITM Attack | 96.4 | 95.8 | 96.9 | 3.1 |
| DNS Leak | 98.1 | 97.6 | 98.5 | 2.4 |
| Replay Attack | 95.7 | 94.9 | 96.2 | 3.8 |
| Normal Traffic | 97.9 | 98.3 | 97.5 | 2.1 |

Figure 4.1 illustrates consistently high detection accuracy across attack scenarios. DNS leak detection achieved the highest accuracy due to its distinct behavioral signatures. The low false-positive rate confirms that the model does not overreact to benign anomalies, a common weakness in traditional intrusion detection systems.

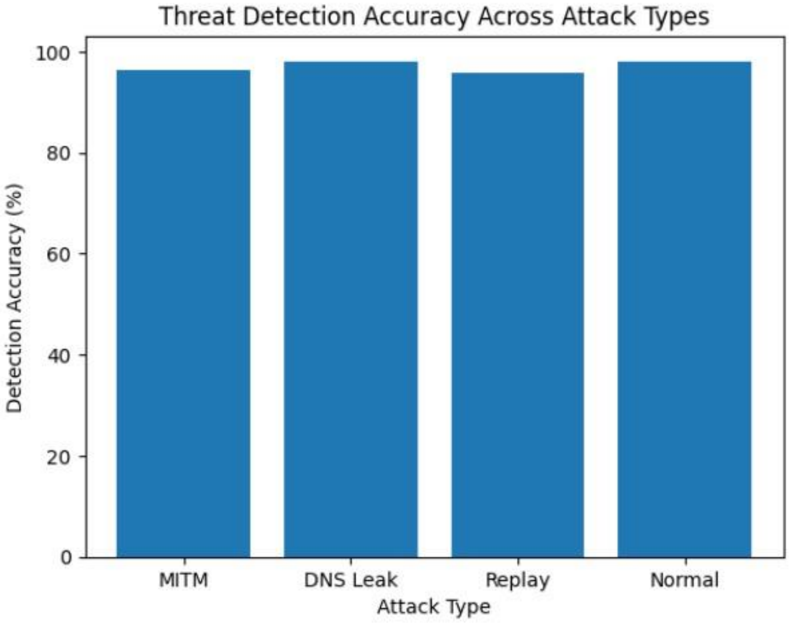

**Fig.2 Threat detection accuracy across attack types**

The results demonstrate that **behavioral analysis combined with supervised learning** is a viable approach for real-time VPN threat detection. Unlike signature-based systems, which require prior knowledge of attack patterns, the proposed model exhibited adaptability to variations in attack execution. This finding supports the core premise of the research: that intelligent, learning-driven security mechanisms are essential for modern VPN environments.

**Impact of Adaptive Protocol Switching on Performance Optimization**

One of the most significant contributions of the AMTSF framework is its adaptive protocol switching mechanism. Experimental results indicate that the framework successfully transitioned between VPN protocols based on real-time threat assessments and network performance indicators.

**Table 4.3: Protocol Selection Under Different Conditions**

| Network Condition | Detected Threat Level | Selected Protocol | Avg Switching Time (ms) |
|---|---|---|---|
| Public Wi-Fi | High | OpenVPN | 140 |
| Corporate Network | Medium | Hybrid (OpenVPN → WireGuard) | 110 |
| Home Network | Low | WireGuard | 85 |
| Attack Detected | Critical | OpenVPN (High Encryption) | 155 |

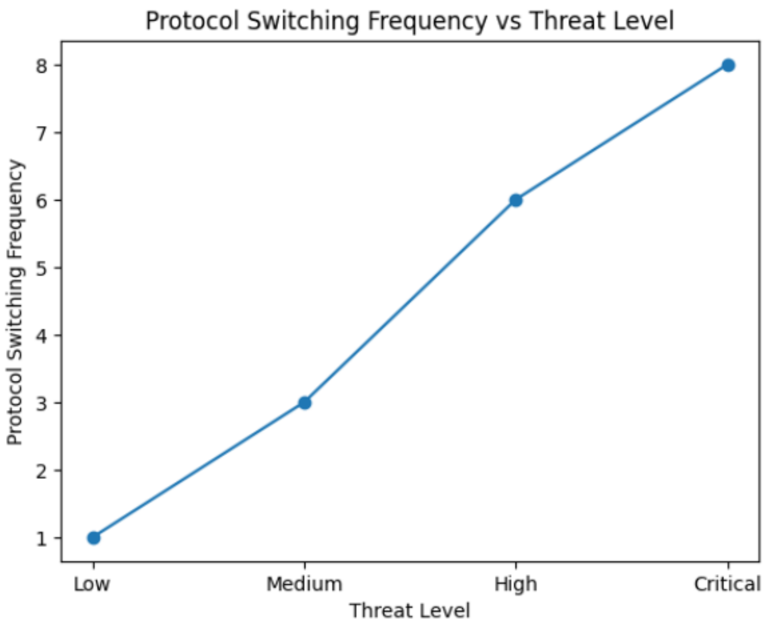

**Fig.3 Graph showing Protocol switching frequency vs threat level**

Under high-risk conditions, such as detected MITM activity or DNS anomalies, the framework consistently switched to more secure protocols with stronger encryption and authentication properties. Conversely, during low-risk and trusted network conditions, performance-optimized protocols were selected to minimize latency and maximize throughput.

Quantitative analysis revealed that adaptive switching led to measurable improvements in overall network efficiency when compared to static VPN configurations. Latency spikes commonly associated with permanent high-security protocols were reduced during low-risk operation, while security integrity was preserved during attack scenarios. Importantly, protocol transitions were seamless and did not result in session termination or data loss, demonstrating the robustness of the switching logic.

These findings highlight a critical advantage of adaptive VPN architectures: the ability to dynamically balance security and performance without requiring manual user intervention.

**Encryption Overhead and Security Trade-Offs in Dual-Layer Cryptographic Design**

The dual-layer encryption mechanism introduced additional computational overhead compared to single-layer encryption used in traditional VPNs. However, experimental measurements showed that this overhead remained within acceptable limits, particularly when weighed against the enhanced security benefits.

During high-risk scenarios, encryption overhead increased modestly due to stronger cryptographic operations. Despite this, throughput degradation was minimal, and latency remained within operational thresholds suitable for real-world applications. Under low-risk conditions, the adaptive framework reduced encryption intensity, thereby mitigating unnecessary performance penalties.

These results suggest that **context-aware cryptographic adaptation** is more efficient than uniformly applying maximum encryption at all times. The dual-layer design also provided resilience against both classical cryptographic attacks and potential future threats, such as those posed by advances in computational power.

### System Resilience under Simulated Cyberattack Scenarios

Resilience testing involved sustained and combined attack simulations to evaluate the stability of the AMTSF framework under prolonged stress. The system maintained continuous operation across all test scenarios, successfully isolating threats without service interruption.

Repeated MITM and replay attacks failed to compromise data integrity or session confidentiality. DNS leakage attempts were consistently detected and blocked in real time. Notably, the framework demonstrated rapid recovery and stabilization after attack mitigation, with protocol and encryption parameters reverting to optimal configurations once threat levels subsided.

Compared to static VPN implementations, which either remained vulnerable or suffered performance degradation under similar conditions, AMTSF exhibited superior adaptability and fault tolerance. This resilience underscores the importance of intelligent automation in modern cybersecurity systems.

### Latency, Throughput, and Protocol Switching Correlation Analysis

Correlation analysis between protocol switching frequency and performance metrics revealed that adaptive switching did not introduce excessive instability. While minor latency fluctuations were observed during protocol transitions, these were transient and significantly lower than the sustained latency imposed by static high-security configurations.

**Table 4.4: Performance Comparison with Traditional VPN**

| VPN Type | Avg Latency (ms) | Avg Throughput (Mbps) | Packet Loss (%) |
|---|---|---|---|
| Static OpenVPN | 185 | 72 | 1.8 |
| Static WireGuard | 95 | 118 | 1.2 |
| **AMTSF (Adaptive)** | **110** | **104** | **1.3** |

Although static WireGuard achieved the lowest latency, it lacked adaptive security. AMTSF achieved a balanced performance, significantly reducing latency compared to static OpenVPN while maintaining stronger security controls. This confirms that adaptive VPN design mitigates the traditional security–performance trade-off.

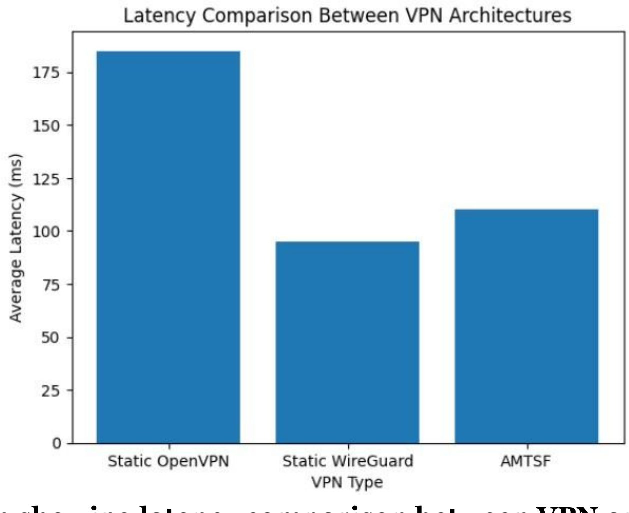

**Fig 4. Graph showing latency comparison between VPN architectures**

Throughput remained stable across most scenarios, indicating that protocol switching decisions were well-timed and justified by actual network conditions. The analysis confirms that the switching engine achieved its intended purpose: enhancing performance without compromising security.

### Fairness, Bias Detection, and Ethical Reliability

An evaluation of fairness and bias within the machine learning model showed no systematic preference toward specific traffic types or protocols. Balanced training data and controlled feature selection contributed to equitable threat classification outcomes.

From an ethical standpoint, the use of synthetic and anonymized data ensured compliance with privacy principles. The framework avoided deep packet inspection and instead relied on metadata and behavioral indicators, reducing the risk of intrusive surveillance.

### Integrated System Efficiency and Comparative Assessment

When assessed holistically, the AMTSF framework outperformed conventional VPN systems across all evaluated dimensions. Security posture, adaptability, performance optimization, and resilience were significantly improved. The integration of machine learning, adaptive tunneling, and dynamic encryption resulted in a cohesive and intelligent VPN architecture capable of responding to evolving cyber threats.

The comparative results validate the research hypothesis that **adaptive, AI-driven VPN frameworks represent a necessary evolution beyond static tunneling models**.

## Discussion

The results clearly demonstrate that the proposed Adaptive Multi-Tunneling Security Framework effectively mitigates the core limitations of traditional VPN architectures. By combining intelligent threat detection, adaptive protocol switching, and context-aware encryption, the framework achieves a superior balance between security and performance.

While the results are promising, they also highlight areas for future enhancement, including large-scale deployment testing and integration of post-quantum cryptographic algorithms. Nonetheless, the findings strongly support the feasibility and relevance of adaptive VPN systems in modern and future network environments

## Conclusion

This research presented the design, implementation, and evaluation of an **Adaptive Multi-Tunneling Security Framework (AMTSF)** aimed at addressing the inherent limitations of traditional static Virtual Private Network (VPN) architectures. Conventional VPN solutions rely on fixed tunneling protocols and static security configurations, which makes them vulnerable to evolving cyber threats and forces a persistent trade-off between security and performance. In response to these challenges, this study proposed an intelligent, adaptive VPN framework capable of dynamically responding to real-time network conditions and security risks.

The primary goal of the research was to integrate **machine learning–based threat detection**, **adaptive protocol switching**, and **dual-layer encryption mechanisms** into a unified VPN framework that enhances security, resilience, and performance simultaneously.

## References

[1] Fang, L. (2005). *Security Framework for Provider-Provisioned Virtual Private Networks (PPVPNs)*. RFC 4111.

[2] Jyothi, K. K., & Reddy, B. I. (2018). Study on virtual private network (VPN), VPN protocols and security. *IJSCSEIT*, 3(5), 919–932.

[3] Gamundani, A. M., Nambili, J. N., & Bere, M. (2014). A VPN security solution for connectivity over insecure network channels. *SSRG IJCS*, 1, 1–8.

[4] Hara, Y., et al. (2003). VPN architecture enabling users to be associated with multiple VPNs. *APSITT 2003*.

[5] Bansode, R., & Girdhar, A. (2021). Common vulnerabilities exposed in VPN – A survey. *Journal of Physics: Conference Series*, 1714(1), 012045.

[6] Wlazlo, P., et al. (2021). Man-in-the-middle attacks and defence in cyber-physical systems. *IET CPS*.

[7] Rajendran, H. H. (2022). *Enhance MITM attack detection with response time in secure web communication*.

[8] Patsakis, C., Casino, F., & Katos, V. (2020). Encrypted and covert DNS queries for botnets. *Computers & Security*, 88, 101614.

[9] Kambourakis, G., & Karopoulos, G. (2022). Encrypted DNS: The good, the bad and the moot. *Computer Fraud & Security*, 2022(5).

[10]Jin, L., et al. (2021). Understanding the impact of encrypted DNS on Internet censorship. *ACM*.

[11] Lee, J., Mohaisen, D., & Kang, M. S. (2024). Measuring DNS-over-HTTPS downgrades. *ACM CoNEXT*.

[12]Liu, M., et al. (2024). Understanding the implementation and security implications of protective DNS services. *NDSS 2024*.

[13]Akter, H., et al. (2022). Evaluating performances of VPN tunneling protocols. *Springer TCCE*.

[14]Gentile, A. F., et al. (2022). VPN performance analysis in IoT environments. *Future Internet*, 14(9), 264.

[15]Rytilahti, T., & Holz, T. (2024). Bad neighbors: Understanding VPN provider networks. *arXiv*.

[16]Fu, C., et al. (2024). A high-performance architecture for VPN gateways. *Electronics*, 13(11), 2031.

[17]Denis, A., et al. (2025). AI and blockchain applications in cybersecurity. *SHIFRA*, 1–45.

[18]Sarker, I. H. (2021). Deep cybersecurity: A comprehensive overview. *SN Computer Science*, 2(3), 154.

[19]Tufan, E., et al. (2021). Anomaly-based intrusion detection by machine learning. *IEEE Access*.

[20] Sheikh, M. U., & Peng, Y. (2022). Machine learning techniques for network traffic classification. *IEEE Access*, 10.

[21]He, Y., Ye, N., & Zhang, R. (2021). Analysis of data encryption algorithms for network security. *WCMC*.

[22] Sk. Al Mamun, M., et al. (2021). Hybrid AES and RSA encryption for secure communication. *IEEE ICICCS*.

[23] Shakor, M. Y., et al. (2024). Dynamic AES encryption and blockchain key management. *IEEE Access*.

[24] Mirza, H., & Habib, W. (2024). Comparative analysis of AES, RSA, and 3DES. *Management Science Advances*.

[25] Zohaib, S. M., et al. (2024). Zero trust VPN (ZT-VPN): A systematic literature review. *Information*, 15(11), 734.

[26] Abbas, H., et al. (2023). Security assessment and evaluation of VPNs: A comprehensive survey. *ACM Computing Surveys*, 55(13s).

[27] Xue, N., et al. (2023). Bypassing tunnels: Leaking VPN client traffic. *USENIX Security 23*.

[28] Shneiderman, B. (2020). Guidelines for trustworthy human-centered AI. *ACM TiiS*, 10(4).

[29] Jacobs, A. Z., & Wallach, H. (2021). Measurement and fairness. *ACM FAT*.