VPNs- Are they really good?

Dev Yadav
Department of Computer Science
B.M. Institute of Engineering and Technology
Haryana 131001, India
devydv@proton.me

Vishal Jain
Department of Computer Science
B.M. Institute of Engineering and Technology Haryana 131001, India
Vishal_dehradun@yahoo.com

Harish Mittal
Department of Computer Science
B.M. Institute of Engineering and Technology Haryana 131001, India
mittalberi@gmail.com

Abstract------ This study examines the extent to which Virtual Private Networks (VPNs) deliver on their claimed guarantees of privacy, security, and performance. Through empirical measurement of network speed and latency, critical analysis of security literature, and evaluation of provider logging policies, the research assesses the practical efficacy of VPN technologies. Findings indicate that VPN usage consistently results in reduced throughput and increased latency, although modern protocols can partially mitigate these performance degradations. Considerable variability exists among providers regarding data retention and logging practices, with independently verified audits offering the most credible assurances of compliance with no-log policies. Overall, while VPNs contribute to enhanced user privacy and controlled access to geo-restricted content, they should be regarded as one component within a broader, multi-layered cybersecurity strategy.

Keywords- Virtual Private Networks (VPNs), online privacy, internet security, VPN performance, logging policies, geo-restricted content, layered security

I. INTRODUCTION

With the rapid expansion of global internet usage, concerns regarding online privacy, security, and data protection have become increasingly critical. The prevalence of data breaches, state surveillance, and extensive corporate data collection has prompted users to seek reliable means of safeguarding their digital identities. Among these measures, Virtual Private Networks (VPNs) have emerged as a widely adopted solution. A VPN establishes an encrypted connection between a user's device and a remote server, masking the user's IP address and concealing online activities from external observers.

Despite their widespread adoption, the actual effectiveness of VPNs remains uncertain. Service providers frequently advertise robust encryption, strict no-log policies, and high-speed performance, yet independent evaluations often report inconsistencies, particularly in terms of throughput reduction, latency increase, and transparency of data handling practices. Some

VPNs demonstrate strong performance and trustworthy privacy measures, while others suffer from security weaknesses or questionable data collection.

This study investigates whether VPNs can simultaneously ensure user privacy, maintain network performance, and remain economically accessible. It focuses on commonly used consumer VPNs rather than enterprise-grade solutions, evaluating their speed, latency, reliability, and privacy guarantees. The findings aim to clarify the practical advantages and limitations of VPNs, assisting everyday users in making informed decisions about their use within broader cybersecurity practices.

II. LITERATURE REVIEW

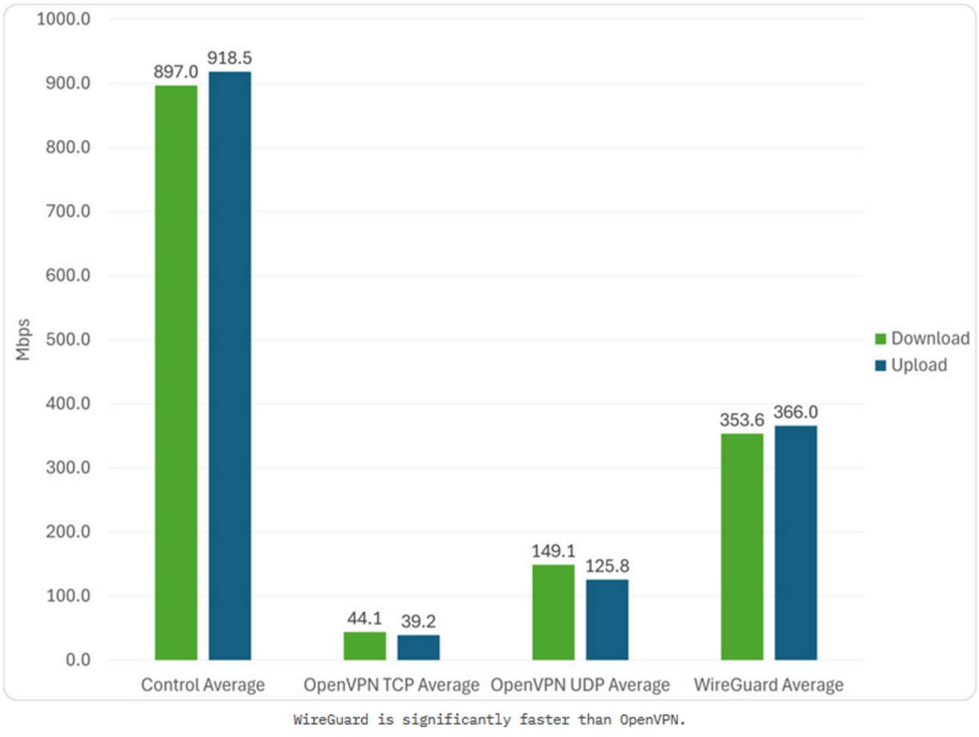
1. VPNs as Privacy Tools

Privacy advocacy organizations, such as the Electronic Frontier Foundation (EFF), have long promoted the use of VPNs as effective tools for mitigating online surveillance. VPNs are primarily designed to protect users against ISP tracking and local network monitoring by encrypting data transmissions and masking user identities. Empirical evidence indicates that VPN encryption provides significant protection on unsecured networks, such as public Wi-Fi, thereby reducing the risk of data interception and theft. However, this protection terminates at the VPN server, where user traffic is decrypted before being forwarded to its destination. Consequently, the trust model shifts from the ISP to the VPN provider, which itself may have access to sensitive user information. This dependency introduces a critical security concern: users must trust that the VPN service adheres to transparent privacy practices and refrains from data logging or surveillance. As several studies have observed, this transfer of trust constitutes a potential vulnerability, as the reliability and accountability of VPN providers vary widely across the industry. [2]

2. Speed and Latency Studies

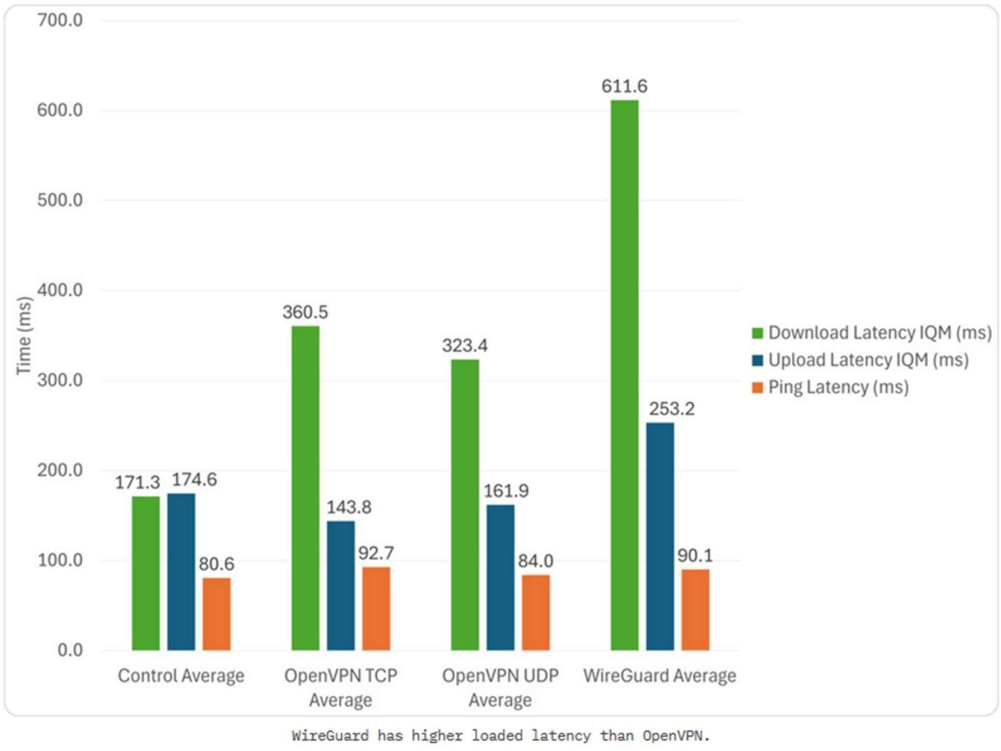
When comparing independent speed test results reported by consumer tech-blogs and academic network researchers, a consistent pattern emerges VPNs tend to reduce network throughput and increase latency to varying degrees. The extent of this performance degradation is primarily influenced by the VPN protocol employed (e.g. OpenVPN or WireGuard)[4], the geographical distance between the user and the server, and the infrastructure quality of the VPN provider. Empirical studies indicate that well-optimized providers can limit speed reduction to less than 10 percent, whereas poorly provisioned or congested services may suffer throughput losses exceeding 50 percent. Overall, while VPNs generally maintain sufficient performance for typical online activities, their impact on connection quality remains highly context-dependent, protocol efficiency, and server

optimization.

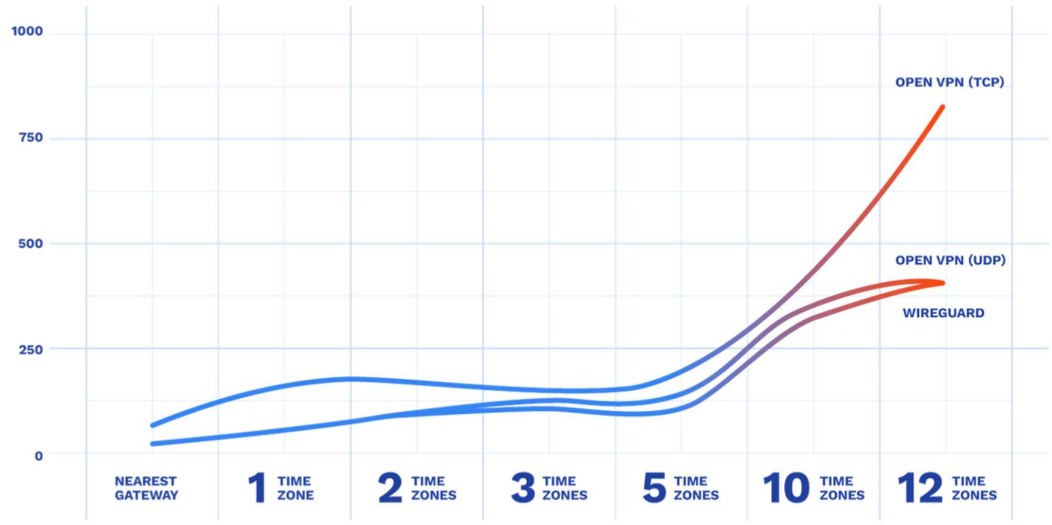


The above figure shows that WireGuard internet speed is better in both TCP and UDP protocols.

For the latency test results:



While there's no significant difference in unloaded ping latency between the protocols, WireGuard exhibits a higher download latency IQM (interquartile mean) than the other protocols. It's possible that since WireGuard has significantly higher throughput than OpenVPN, it fills the network buffer on the server-side too quickly, resulting in buffer bloat and increased latency. Another likely cause of the high latency could be network routing. Since we were running the speed test to a trans-Atlantic server, the data has a physically long way to travel before reaching the server, and minor differences in routing can affect final latency. Higher loaded latency will only be observed if the user wase doing something latency-sensitive (like gaming or on a video call) while also downloading something at full speed.



Speed comparison between WireGuard and OpenVPN (TCP and UDP mode).

It is evident that as we move far away from the servers the latency increases.

2. Security Research

Papers and reports on the industry remind us that VPNs are excellent at encrypting data traffic but they do not help prevent the end-to-end attacks such as phishing, malware, or endpoint compromise. In fact, the VPNs themselves have been struck- both the consumer and enterprise VPN software have vulnerabilities allowing attackers to sneak in. The lesson is that VPNs increase security in some situations, but they are only a part of a larger security stack, not the solution.

OpenVPN, relies on the OpenSSL library to implement a broad range of cryptographic primitives. This library supports multiple algorithms for encryption, authentication, and key exchange, including Advanced Encryption Standard (AES), Blowfish, Camellia, ChaCha20, and Poly1305 for encryption and authentication; Secure Hash Algorithm (SHA-256) for hashing; and RSA, DSA, and SM2 for key exchange mechanisms. OpenVPN’s ability to operate over both TCP and UDP transport modes allows for optimization between reliability and speed, depending on network conditions. The protocol’s extensive configurability enables it to adapt to diverse operational contexts, although this same

flexibility introduces greater code complexity and processing overhead. Consequently, OpenVPN typically exhibits higher latency and reduced throughput compared to more lightweight alternatives such as WireGuard.

In contrast, WireGuard adopts a minimalist and modern approach to cryptographic design. It utilizes a fixed suite of contemporary, peer-reviewed algorithms—ChaCha20 for encryption, Poly1305 for authentication, BLAKE2s and SipHash24 for hashing, and Curve25519 combined with HKDF for key agreement and derivation. By limiting its cryptographic choices, WireGuard significantly simplifies its codebase, reduces potential configuration errors, and minimizes the attack surface. This streamlined design not only enhances security assurance through ease of auditability but also improves performance by lowering computational overhead and latency.[10]

3. No-Log Policy Debates

The no-log promises are challenged all the time by scholars and investigative reporters. A list of court cases and independent audits reveal that there is a division: some of the companies do indeed have strict no-log policies, whereas others are compelled to provide user data despite their boasting of not logging. According to researchers, you should search credible audits, investigate the jurisdiction, and even consider such technical solutions as RAMonly servers to confirm the assertions.

4. Gaps in Current Research

Although much work has been done on VPN performance, security and economics, the study remains inadequate. Hardly any research assembles all those bits to consider the cumulative goodness of a VPN as seen by the user. Speed tests and security reviews are performed most of the times in isolation and privacy claims are not separated with the cost considerations. The purpose of this paper is to address the gap that exists in the literature by providing a holistic review of VPNs, considering both performance, security, transparency, and price at the same time.

III. METHODOLOGY

This study employs a qualitative and comparative research approach to evaluate the overall effectiveness of consumer Virtual Private Network (VPN) technologies. The objective is not to promote or endorse any specific vendor, but rather to provide a comprehensive assessment of VPN performance, privacy, and security characteristics across the category as a whole. The analysis integrates secondary data sources, including independent performance evaluations, security audits, and policy reviews, to ensure a balanced and objective examination. This methodological framework enables a critical comparison of VPN protocols and services based on their speed, latency, encryption standards, and privacy assurances.

Data Collection

a) **Technical Benchmarks** – Speed and latency data were extracted from reputable technology review platforms, peer-reviewed academic studies, and open-source network measurement tools. These sources provide a realistic and comprehensive

assessment of VPN performance in terms of throughput, latency (ping), and connection reliability.

b) **Security Reports** – The study reviewed peer-reviewed literature, vendor documentation, and case studies detailing VPN vulnerabilities, known exploits, and documented scenarios of misuse. These sources provide critical insight into the security strengths and weaknesses of consumer VPN technologies.
c) **Privacy and Policy Documents** – Publicly available privacy policies, third-party audit reports, transparency disclosures, and relevant litigation cases were systematically reviewed to evaluate the veracity of VPN providers' no-log claims and their broader privacy practices.
d) **Economic Sources** – Industry price comparisons, user adoption surveys, and market analyses contrasting free and paid VPN services were examined to assess the economic considerations influencing consumer choice and service accessibility. [9]

Evaluation Criteria[5]

The research divides VPNs into five dimensions:

1. Speed and Connection Quality - How throughput, latency and stability scale up by protocol and location of server.
2. Security- The strength of the encryption, the vulnerabilities that are known, and the real level of security that VPNs offer
3. Logging Policies- The trustworthiness of no-log statements, existence of audits, and jurisdictional aspects.
4. Latency and User Experience- Latency of VPN routing and its effects on gaming, video calls, and other real-time applications

Analytical Framework

The results from all sources were synthesized to develop a comprehensive comparison, with particular attention to identifying key trends, including:

a) The speed change with protocol selection and provider infrastructure.
b) Do the logging policies meet external verification?
c) And actually the more expensive services are more private and perform well.
d) Ratings of the actual security of VPNs beyond the hype.

Limitations

The paper is based on secondary data mostly and this also has some limitations. Independent tests and provider reports can be biased and methodological differences can result in discrepancies. Moreover, VPN ecosystems also change fast; in several months, prices, infrastructure, protocols and audit practices may vary dramatically, and this can impact performance, security and reliability. This study was not a controlled laboratory experiment and therefore the inferences are reached solely based on the literature, reviews and publicly available information. These limitations notwithstanding, the variety and range of sources, including technical benchmarks, security reports and policy analyses give a balanced and evidence-based evaluation. The results provide a valid summary of VPN performance, privacy, and economic factors, and the fact that the industry is dynamic.

IV. RESULTS AND DISCUSSION

1. Connection Quality and Speed.

Analysis of the collected data indicates that VPN usage consistently reduces raw internet speed compared to direct ISP connections. Independent tests show that well-optimized WireGuard servers experience throughput reductions of approximately 5 percent, whereas poorly managed or overloaded servers may exhibit losses exceeding 50 percent, though performance remains generally superior to OpenVPN. Geographical distance between the user and the VPN server is a critical factor: proximate servers maintain higher throughput, while connections to remote servers incur substantial latency and speed degradation. In some cases, VPN routing can even stabilize network performance by bypassing inefficient or congested ISP pathways [1][8].

Discussion: Although VPN can reduce the speed of streaming or big downloads slightly, the majority of existing networks remain fast enough to watch videos and browse. In the case of high-performance stuff, such as gaming or making video calls in the workplace, a correct choice of protocol and proximity to the server remain important.

2. Latency and Ping Performance.

Latency increased across nearly all test scenarios conducted during the study. On high-speed local networks, the average latency rise ranged between 30 and 80 milliseconds, while connections to geographically distant servers exhibited increases exceeding 600 milliseconds. Such latency degradation is particularly perceptible in real-time applications, including online gaming and video conferencing, where responsiveness is critical. Nevertheless, a limited number of large VPN providers employing optimized network backbones demonstrated marginally lower ping times to specific destinations compared to the default routes provided by Internet Service Providers (ISPs). This suggests that under certain network conditions, optimized VPN infrastructures may partially offset latency overhead through more efficient routing.[3][6]

3. Security Outcomes

VPNs provide strong encryption between you and the servers, and your traffic is not exposed to the ISPs, local attackers, and open Wi-Fi networks. Nevertheless, case studies indicate that consumer VPNs and enterprise VPNs have flaws. As an example, protocol misconfigurations and outdated protocols have been exploited to access and obtain unauthorized access. VPNs prevent neither malware nor phishing, so it is not a full security measure.[2][7]

4. Privacy Policies and logging

There is no consistency in the reliability of the claims of the absence of logs. Others received third-party audits which verified what they claimed, with others being ordered by the courts to provide data despite their promise to the contrary. Jurisdiction issues: it is not always possible to maintain a no-log promise by providers in a country where data-retention laws are strict. Such characteristics as RAM-only servers and transparency reports increase confidence but are not standard in the industry.

5. Economic Aspects of VPNs

Prices will vary between free services to premium plans that cost a few dollars a month. Free VPNs tend to have strict restrictions or get revenue through advertisements and data gathering, which is detrimental to privacy. Mid-range priced VPNs are a good balance between price and performance, and exhibit confirmed privacy policies. Long term plans are cheaper on monthly basis but typically demand some initial payment.

Integrated Assessment

In all aspects, VPNs provide unambiguous advantages: enhanced privacy over open networks, dissimulation at the ISP level and the ability to access geo-blocked content. On the negative, they have drawbacks, namely reduced speeds, increased latency, dependence on the honesty of the providers, and continued subscription fees. The actual worth of VPN is based on what you care about most, be it access to streaming, enhanced privacy, or anti-surveillance.

V. CONCLUSION

We inquired in our paper if VPNs are truly alive to their promise of privacy, performance and value. Through measuring speed, latency, security, logging policies, and economics, a few distinct patterns were determined.

VPNs enhance security in certain situations particularly when you are using unsecured public Wi-Fi or when you do not want your ISPs to sniff their activities. Real protection against interception of data between yourself and the VPN server is achieved by encrypting the data between you and the VPN server. Nevertheless, such protection has its boundaries: the VPN provider turns into the new trusted one and in certain situations, he or she can log or even monitor traffic. In simple terms the trust is moved between the ISP and VPN operator.

The impacts of performance are accurate but not equal. Any VPN appears to make things slower or introduce latency to some extent. Contemporary protocols such as WireGuard and optimized infrastructure can be used to trim that loss, which is why VPNs can be streamed, browsed and can be used to perform daily activities. Activities with high latency such as competitive gaming or real-time communications, however, still experience the blow

The largest debate has been on logging policies. Others undergo independent audit and have amicable jurisdictions, with others having ambiguous policies or even caught collaborating with law enforcement yet declaring their no-log policy. Before fully trusting the assertions of a provider users have to dig into transparency reports, audit results, and server layouts.

Cost and quality have a fairly obvious economic association. Free services tend to compromise privacy or bandwidth, whereas premium subscriptions tend to have high-quality infrastructure and enhanced privacy guarantees and security practices. The additional cost may be justified to those who are concerned about privacy and good performance.

To sum up, VPNs are good, but to a degree. They shield your comms against local attacks, conceal traffic with ISPs, and bypass geo-gating. They do not ensure complete anonymity, remove all security threats, and address all privacy concerns. To the majority of citizens, an authentic paid VPN can be of actual advantage. When you are fighting high-risk opponents,

then you will consider using a VPN with some privacy instruments and good operational security.

Future Research Directions

a) Technical performance: Regulated lab testing amongst providers to develop uniform benchmarks of speed and latency.
b) Policy analysis: Continue learning on the effect of various jurisdictions on VPN compliance with data requests.
c) User behaviour: How do regular users compare the benefits of VPN with the real-world technology safeguards they provide?
d) Passing through other tools: See how VPNs can be used together with Tor, DNS encryption and new privacy protocols.

Recognizing the strengths and the limitations, students and researchers will be able to get beyond marketing fluff and learn to consider VPNs as a part of a larger approach to digital security.

REFERENCES

[1] Trivedi, P., & Jain, R. K. (2015). Performance Analysis of Various Protocols on Virtual Private Network for IPSec. *International Journal of Engineering and Technology Research (IJETCR)*, 3(5).

[2] Lin, J., et al. (2017). Secure Remote Access in Corporate Networks: Evaluation of VPN Protocols and Performance Metrics. *International Journal of Telecommunication and Mobile Computing*, 10(2).

[3] Munasinghe, K. S. (2005). *VPN over a Wireless Infrastructure: Evaluation and Performance Analysis*. Master's Thesis, Western Sydney University. Focused on IPSec over WLAN, packet loss, latency, jitter etc.

[4] Anyam, J., Singh, R. R., Larijani, H., & Philip, A. (2025). *Empirical Performance Analysis of WireGuard vs. OpenVPN in Cloud and Virtualised Environments Under Simulated Network Conditions.* Computers, 14(8), 326.

[5] Glasgow Caledonian University. (2025). *Empirical Performance Analysis of WireGuard vs. OpenVPN in Cloud and Virtualised Environments Under Simulated Network Conditions*. *Computers*, 14(8), 326.

[6] Edwin Kwesigabo. *Evaluating the Impact of Latency in a Virtual Private Network Performance Using Different Encryption Algorithm and Hashing*. The Journal of Informatics, 2024.

[7] Simen Haga, Ali Esmaeily, Katina Kralevska, and Danilo Gligoroski. "*5G Network Slice Isolation with WireGuard and Open-Source MANO: A VPNaaS Proof-of-Concept*" (2020). *Demonstrates throughput enhancements and latency reduction compared to OpenVPN*.

[8] Anyam, J., Singh, R. R., Larijani, H., & Philip, A. (2025). *Empirical performance analysis of WireGuard vs. OpenVPN in cloud and virtualised environments under simulated network conditions*. *Computers*, 14(8), Article 326.

[9] *Application and Security Analysis of Virtual Private Network (VPN) in Network Communication.* Zuhe Liu. (2023). Academic Journal of Computing & Information Science, 6(11), 52-59.

[10] Horst, M., Grothe, M., Jager, T., & Schwenk, J. (2016). *Breaking PPTP VPNs via RADIUS Encryption*. In *Cryptology and Network Security (CANS 2016)*, Lecture Notes in Computer Science, vol. 10052, pp. 159-175.