PT Mekar Research and Publishing
MIKIR : Mathematics, Informatics, Knowledge And Information Research
ISSN : 3110-7699 (Online)
Url : https://mikir.org/mikir

Analysis of Virtual Private Network (VPN) Protocols, Security, and Performance in the IPv6 Transition Ecosystem

Livia Rialta Armadany[1], Romy Indra Gotama[1], Rifan Eka Aditya Arputra[1]
[1] Teknik Informatika, Universitas Muhammadiyah Ponorogo
Jl Budi Utomo No 10 Ponorogo, Indonesia
*Corresponding Author Email: liviarialta@gmail.com

Doi : https://doi.org/10.65475/3jf1c064

Key-Words :
Digital Privacy, VPN, IPv6, Network Security, Data Protection.

Received : May 3, 2026.
Revised : May 10, 2026.
Published : May 30, 2026

Abstract

Amidst increasingly rapid technological advancements, maintaining digital privacy is no longer merely an option, but a fundamental necessity for every individual. As the world transitions to IPv6 infrastructure to accommodate billions of new devices in the internet ecosystem, the challenge of safeguarding personal information is growing. This paper examines how Virtual Private Network (VPN) technology has emerged as a primary safeguard for users in maintaining the confidentiality of their identities and data in open public spaces. Through a review of various literature, this paper examines the evolution of network security technology—from classic protocols to modern innovations like WireGuard, which offer more efficient protection without sacrificing speed. Beyond discussing technical advantages, this paper also highlights human vulnerabilities, such as the risk of data leaks that users often fail to recognize during network transitions.The analysis shows that while technology continues to advance toward intelligent automation and artificial intelligence, true security can only be achieved through a combination of robust protocols and a sound understanding of future risks. In conclusion, strengthening the relationship between VPN and IPv6 is a crucial step towards creating a safer, more convenient, and more humane digital environment for everyone in the long term.

1. INTRODUCTION

Di tengah laju peradaban digital yang kian cepat, internet bukan lagi sekadar alat, melainkan ruang tempat menitipkan sebagian besar aktivitas, rahasia, dan identitas diri. Seiring dengan pertumbuhan jumlah pengguna dan perangkat yang saling terhubung, fondasi internet lama yang kita kenal sebagai IPv4 mulai terasa sempit dan rentan. Keterbatasan ruang ini memaksa kita untuk beralih ke rumah baru yang lebih luas dan canggih yaitu IPv6. Namun, perpindahan ke wilayah baru ini membawa ketidakpastian dan tantangan keamanan yang sering kali membuat terasa tidak terlindungi di ruang siber yang luas. Kehadiran Virtual Private Network (VPN) muncul sebagai bentuk ikhtiar manusia untuk menciptakan rasa aman di tengah keramaian jaringan publik. VPN bukan hanya sekadar barisan kode dan enkripsi, melainkan sebuah pelindung yang memastikan bahwa percakapan dan data pribadi tetap menjadi milik tiap pengguna sepenuhnya. Di masa transisi menuju infrastruktur internet yang lebih modern, memahami bagaimana VPN bekerja dan melindungi pengguna adalah langkah krusial. Pengguna dihadapkan pada pilihan teknologi, mulai dari protokol yang mapan hingga inovasi baru yang lebih efisien, yang semuanya bertujuan satu, yaitu menjaga integritas kemanusiaan di dunia maya.

Tinjauan literatur ini disusun untuk menyelami dinamika hubungan antara privasi dan teknologi. Peneliti akan mengeksplorasi bagaimana mekanisme pertahanan digital ini beradaptasi dengan perubahan protokol internet, menghadapi ancaman kebocoran data yang tidak terlihat, hingga mempersiapkan diri menyongsong masa depan yang serba otomatis. Pada akhirnya, pembahasan ini mengajak pembaca untuk melihat teknologi bukan sebagai entitas yang dingin, melainkan sebagai kawan yang memastikan bahwa di tengah arus data yang tak terbatas, privasi dan keamanan setiap individu tetap terjaga dengan terhormat

2. METHODS

Penyusunan tinjauan literatur ini dilakukan melalui pendekatan yang menyeluruh untuk memahami keterkaitan antara keamanan jaringan dan perkembangan teknologi internet. Langkah awal dimulai dengan mengumpulkan berbagai karya ilmiah, jurnal teknis, serta laporan penelitian yang relevan dari berbagai sumber digital. Fokus utama pencarian diarahkan pada topik yang mencakup teknologi VPN, infrastruktur IPv6, serta berbagai tantangan privasi yang muncul di era transisi digital saat ini.

Setelah data terkumpul, dilakukan proses pemilihan yang cermat untuk memastikan bahwa setiap sumber yang digunakan memiliki keterkaitan yang kuat dengan topik bahasan. Informasi yang didapat kemudian dikelompokkan ke dalam beberapa bagian utama, mulai dari pemahaman mendasar mengenai arsitektur jaringan, perbandingan teknis antarprotokol VPN seperti WireGuard dan OpenVPN, hingga evaluasi mendalam terhadap risiko kebocoran data.

Analisis dilakukan dengan cara menyandingkan berbagai temuan penelitian untuk mendapatkan gambaran yang utuh mengenai kelebihan serta kekurangan dari setiap teknologi yang dibahas. Proses ini bukan sekadar mengumpulkan fakta teknis, melainkan sebuah upaya untuk merangkai pemikiran agar dapat memberikan pandangan yang jernih mengenai arah masa depan keamanan siber. Dengan cara ini, setiap simpulan yang diambil diharapkan dapat menjadi landasan yang kokoh bagi pemahaman mengenai perlindungan privasi manusia di tengah kompleksitas dunia maya yang terus berubah.

3. RESULTS AND DISCUSSION

3.1 Fondasi Keamanan dan Transformasi Jaringan

Di era di mana hampir seluruh aspek kehidupan manusia berpindah ke ruang siber, perlindungan terhadap identitas digital telah menjadi sebuah kebutuhan yang sangat mendasar. Teknologi VPN hadir sebagai bentuk upaya kolektif untuk menciptakan jalur komunikasi yang aman melalui enkripsi data, yang bertujuan untuk melindungi privasi kita saat berada di jaringan publik yang sering kali memiliki kontrol keamanan yang rendah [1]. Keberhasilan komunikasi ini tidak terlepas dari peran sistem DNS yang bekerja dengan cara menerjemahkan alamat yang mudah diingat oleh manusia menjadi deretan angka protokol internet yang rumit, sehingga data dapat terkirim dengan tepat dan andal [2]. Namun, kita harus menyadari bahwa fondasi internet lama yang kita gunakan selama puluhan tahun, yaitu IPv4, kini sudah mencapai batas maksimalnya dan menyimpan banyak kerentanan yang memudahkan pihak lain untuk melakukan penyusupan [3]. Sebagai gantinya, IPv6 hadir dengan kapasitas yang jauh lebih luas serta fitur keamanan yang lebih matang untuk mendukung ekosistem teknologi masa depan [4]. Dalam masa transisi yang penuh tantangan ini, mekanisme seperti DNS64 dan NAT64 dikembangkan agar perangkat yang berbeda generasi tetap bisa saling terhubung dengan baik [5]. Dukungan dari teknologi Dual Stack dan Tunneling juga memastikan bahwa proses pemindahan data tetap berjalan lancar tanpa hambatan berarti [6]. Meskipun berbagai metode seperti 6to4 dan Teredo memberikan kemudahan dalam migrasi [7], kita tetap perlu memperhatikan bagaimana mekanisme ini memengaruhi efisiensi dan beban kerja sistem secara keseluruhan agar tidak merugikan pengguna [8].

3.1 Evolusi Protokol VPN dan Kekuatan Pelindungnya

Seiring dengan meningkatnya kesadaran akan privasi, berbagai protokol VPN terus berkembang untuk menawarkan perlindungan yang lebih kuat bagi setiap individu [9]. Salah satu inovasi yang paling menonjol adalah WireGuard, yang melalui kesederhanaan desainnya mampu memberikan kecepatan tinggi serta penggunaan daya yang lebih hemat, menjadikannya pilihan yang sangat ramah bagi perangkat modern [10]. Sementara itu, OpenVPN tetap memegang peranan penting sebagai standar keamanan yang dipercaya oleh banyak pihak karena sifatnya yang transparan dan mudah disesuaikan dengan berbagai kondisi jaringan [11]. Bagi mereka yang sering bepergian, protokol IKEv2 memberikan rasa tenang yang luar biasa karena kemampuannya dalam menjaga koneksi tetap stabil meskipun perangkat berpindah-pindah dari satu jaringan ke jaringan lainnya [12]. Seluruh sistem ini diperkuat oleh algoritma enkripsi AES 256 yang secara teknis sangat tangguh, sehingga memberikan rasa aman yang nyata bagi siapa pun yang ingin melindungi informasi pribadi mereka dari upaya peretasan [13].

3.2 Tantangan Privasi di Tengah Celah Keamanan

Perjalanan menjaga privasi digital ternyata tidak selalu mulus, karena masih terdapat celah-celah kecil yang sering kali tidak terlihat oleh mata pengguna. Risiko kebocoran data melalui sistem DNS atau alamat IP tetap menjadi ancaman serius yang dapat mengungkap identitas kita secara tidak sengaja [14]. Sebagai langkah antisipasi, fitur Kill Switch hadir sebagai garda terdepan yang akan langsung menutup seluruh akses internet apabila perlindungan VPN terputus, sehingga tidak ada satu pun informasi yang keluar ke ruang publik tanpa perlindungan [15]. Selain teknologi, aspek kepercayaan juga menjadi sangat penting, di mana kejujuran penyedia layanan untuk benar-benar menjalankan kebijakan tanpa catatan aktivitas menjadi janji yang harus ditepati demi menjaga martabat privasi pengguna [16]. Kita juga didorong untuk menggunakan teknologi enkripsi jalur pencarian internet agar terhindar dari pengintaian oleh pihak-pihak yang ingin mengambil keuntungan dari data navigasi kita [17]. Hal ini menjadi semakin krusial mengingat adanya potensi kerentanan pada protokol yang mengatur komunikasi antar perangkat di sekitar kita [18], serta bahaya pembajakan sistem navigasi yang dapat menyesatkan arah komunikasi digital ke tempat yang berbahaya [19].

3.3 Kinerja Teknis dan Pengalaman Pengguna

Dalam penggunaan sehari-hari, kita sering kali merasakan beban teknologi pada perangkat yang kita gunakan, seperti konsumsi baterai yang lebih cepat habis atau suhu perangkat yang meningkat saat menjalankan sistem keamanan yang berat [20]. Masalah teknis seperti terpecahnya paket data di tengah jalur komunikasi juga menjadi tantangan yang dapat mengganggu kenyamanan kita saat sedang bekerja atau berkomunikasi [21]. Namun, hasil penelitian memberikan kabar yang menggembirakan bahwa penggunaan VPN pada jaringan IPv6 ternyata

mampu memberikan kecepatan pengiriman data yang lebih baik dibandingkan dengan cara-cara lama [22]. Walaupun terkadang terdapat sedikit jeda waktu dalam merespons perintah [23], penyesuaian yang tepat pada pengaturan ukuran paket data dapat membantu kita mendapatkan pengalaman berselancar yang lebih nyaman dan lancar [24]. Kita perlu memahami bahwa setiap lapisan keamanan tambahan memang akan memberikan sedikit beban pada lalu lintas data, namun itu adalah harga yang pantas dibayar demi mendapatkan perlindungan yang maksimal [25].

3.4 **Masa Depan Keamanan dan Kecerdasan Buatan**

Menyongsong masa depan, teknologi VPN kini mulai dikembangkan untuk dapat bekerja secara lebih cerdas, seperti kemampuan untuk memilih server terbaik secara otomatis berdasarkan kebutuhan unik setiap pengguna [26]. Selain itu, terdapat upaya untuk menyamarkan jalur komunikasi agar orang-orang yang berada di wilayah dengan pengawasan ketat tetap dapat terhubung dengan dunia luar secara bebas, meskipun hal tersebut menuntut pengorbanan pada sisi kecepatan [27]. Fokus utama pengembangan ke depan adalah bagaimana kita dapat menemukan keseimbangan yang sempurna antara keamanan yang tidak tertembus dan efisiensi yang membuat teknologi tetap nyaman digunakan oleh siapa pun [28]. Kita dituntut untuk bijak dalam menimbang antara tingkat perlindungan terhadap sensor dengan kemampuan sistem dalam mengirimkan data secara optimal [29]. Pada akhirnya, kita harus bersiap menghadapi kemajuan komputer masa depan yang sangat kuat yang mungkin mengancam sistem keamanan saat ini, sembari terus memanfaatkan kecerdasan buatan untuk menjaga agar dunia digital tetap menjadi tempat yang aman dan manusiawi bagi kita semua [30].

4. CONCLUSION

Perjalanan peneliti dalam menelaah berbagai literatur ini membawa pada satu pemahaman penting bahwa teknologi sebenarnya adalah alat untuk menjaga martabat dan privasi manusia. Di tengah laju perpindahan dunia digital menuju infrastruktur IPv6 yang lebih luas, peneliti melihat bahwa keamanan bukan lagi sekadar pilihan teknis, melainkan sebuah kebutuhan batin agar setiap individu merasa tenang saat berinteraksi di ruang siber. Kehadiran Virtual Private Network (VPN) telah membuktikan perannya sebagai pelindung yang setia, yang memastikan bahwa identitas dan rahasia pribadi kita tetap terjaga meskipun kita berada di tengah jaringan publik yang terbuka.

Peneliti juga menyaksikan bagaimana inovasi terus lahir untuk menjawab kebutuhan manusia akan kecepatan dan efisiensi. Evolusi dari protokol lama menuju teknologi yang lebih modern seperti WireGuard menunjukkan bahwa keamanan yang kokoh tidak harus terasa berat atau membebani perangkat pengguna. Namun, di balik kecanggihan tersebut, pengguna diingatkan bahwa kewaspadaan terhadap celah-celah kecil seperti kebocoran data tetap menjadi kunci utama. Pada akhirnya, integritas sebuah sistem keamanan sangat bergantung pada perpaduan antara keunggulan teknologi dan kejujuran dari para penyedia layanan dalam menjaga amanah data penggunanya.

5. **SUGGESTION**

Demi menciptakan lingkungan digital yang lebih aman dan nyaman bagi pengguna di masa depan, ada beberapa langkah bijak yang dapat menjadi perhatian bersama. Pertama, bagi para pengembang dan penyedia layanan keamanan, kiranya aspek transparansi dan kemudahan penggunaan harus selalu diutamakan, sehingga teknologi perlindungan ini dapat menjangkau dan dipahami oleh semua kalangan tanpa terkecuali. Kejujuran dalam menjaga kebijakan tanpa catatan aktivitas adalah fondasi utama untuk membangun kepercayaan jangka panjang dengan pengguna.

Kedua, sebagai pengguna internet, sangat penting untuk tidak hanya mengandalkan teknologi secara buta, tetapi juga terus membekali diri dengan pemahaman mengenai risiko digital yang mungkin terjadi, seperti potensi kebocoran jalur navigasi saat berada di jaringan baru. Terakhir, bagi para peneliti dan praktisi teknologi, sangat disarankan untuk terus menggali potensi kecerdasan buatan dan sistem enkripsi masa depan yang tahan terhadap ancaman komputer super cepat. Dengan terus melakukan inovasi yang berorientasi pada perlindungan manusia, kita dapat memastikan bahwa kemajuan teknologi akan selalu berjalan selaras dengan upaya menjaga privasi dan kehormatan setiap individu di dunia maya.

REFERENCES

[1] S. N. A. S. Freenas, M. Affandi, F. Teknik, and U. Tanjungpura, “Jurnal Impresi Indonesia (JII) IMPLEMENTASI VIRTUAL PRIVATE NETWORK (VPN) OPEN VPN DENGAN KEAMANAN SERTIFIKAT SSL PADA NETWORK ATTACHED,” vol. 1, no. 12, 2022.

[2] J. Burrell, “Special issue on domain name system (DNS),” vol. 8871, no. 2023, 2024, doi: 10.1080/23738871.2024.2312922.

[3] M. Ndclm, “Implementasi Dan Evaluasi Perbandingan IPV4 dan IPV6,” vol. 14, no. 1, pp. 91–103, 2025, doi: 10.36774/jusiti.v14i1.1542.

[4] F. Mauren, N. Hura, A. D. Lase, and D. C. Lase, “Penerapan Virtual Privat Network (VPN) untuk Keamanan Data,” vol. 4, no. 3, pp. 2357–2366, 2026.

[5] T. Barbette, N. Rybowski, C. Pelsser, and F. Michel, “The multiple roles that IPv6 addresses can play in today ’ s Internet,” vol. 52, no. 3, pp. 10–18, 2022.

[6] J. Schwenk, “IP Security (IPsec),” in *Guide to Internet Cryptography: Security Protocols and Real-World Attack Implications*, Cham: Springer International Publishing, 2022, pp. 135–190. doi: 10.1007/978-3-031-19439-9_8.

[7] H. Abbas, N. Emmanuel, and M. F. Amjad, “Security Assessment and Evaluation of VPNs : A Comprehensive Survey,” vol. 55, no. 13, 2023.

[8] Sura Ghanim Hussein and Syed Muhammad Fasih Ur Rehman, “Protocol Efficiency and Resource Utilization in VPN Technologies: A Comparative Analysis of OpenVPN and WireGuard,” *J. Tech.*, vol. 7, no. 4 SE-Engineering (Miscellaneous): Computer Engineering, pp. 37–42, Dec. 2025, doi: 10.51173/jt.v7i4.2768.

[9] Z. Ali, “Evaluation of AES-256 encryption and machine learning for securing GSM communications against sniffing attacks,” *Egypt. Informatics J.*, vol. 32, no. November, p. 100832, 2025, doi: 10.1016/j.eij.2025.100832.

[10] I. Farooq, S. A. Ahmed, A. Ali, M. A. Warraich, M. Aqeel, and H. Khan, “Enhanced Classification of Networks Encrypted Traffic : A Conceptual Analysis of Security Assessments , Implementation , Trends and Future Directions,” vol. 4, 2024.

[11] W. Wang *et al.*, “MVPNalyzer: An Investigative Framework for Auditing the Security \& Privacy of Mobile VPNs,” in *The Network and Distributed System Security Symposium*, 2026.

[12] D. El Khaled, R. AlOtaibi, N. Novas, and J. A. Gazquez, “NetworkGuard: An Edge-Based Virtual Network Sensing Architecture for Real-Time Security Monitoring in Smart Home Environments,” *Sensors*, vol. 26, no. 7, 2026, doi: 10.3390/s26072231.

[13] M. Liu *et al.*, “Understanding the Implementation and Security Implications of Protective DNS Services,” no. March, 2024.

[14] 석상윤, “CertDNS: DNS Security Using Digital Certificate TT - 전자인증서를 활용한 DNS 보안 연구 TA - Sangyoon Seok,” 서울대학교 대학원, 2022. [Online]. Available: https://hdl.handle.net/10371/181055

[15] K. Hynek and A. Wasicek, *Large Scale Measurement on the Adoption of Encrypted DNS*, vol. 1, no. 1. Association for Computing Machinery, 2021.

[16] C. Kwan, P. Janiszewski, S. Qiu, and C. Wang, “Exploring Simple Detection Techniques for DNS-over-HTTPS Tunnels,” pp. 37–42, 2021.

[17] A. Al-azzawi, “Analysis of the Security Challenges Facing the DS-Lite,” 2023.

[18] M. Bach, L. Knittel, R. Merget, and J. P. Degabriele, “Analyzing the WebRTC Ecosystem and Breaking Authentication in DTLS-SRTP,” 2021.

[19] N. Venkata, S. Korlapati, F. Khan, Q. Noor, and S. Mirza, “Journal of Pipeline Science and Engineering,” vol. 2, no. March, 2022, doi: 10.1016/j.jpse.2022.100074.

[20] A. Zilberman, A. Dvir, and A. Stulman, “IPv6 Routing Protocol for Low-Power and Lossy Networks Security Vulnerabilities and Mitigation Techniques : A Survey,” vol. 57, no. 11, 2025.

[21] T. Wang, *Research on the application of DNS64 / NAT64 technology in IPv6 environment in national network security*, vol. 1, no. 1. Association for Computing Machinery, 2025. doi: 10.1145/3727505.3727526.

[22] K.-H. Li and K.-Y. Wong, “Empirical Analysis of IPv4 and IPv6 Networks through Dual-Stack Sites,” 2021. doi: 10.3390/info12060246.

[23] I. Shafinaz, A. Razak, A. Razak, P. Tuanku, S. Bahiyah, and K. H. Park, “ANP A Comparative Study between IPv4 and IPv6,” vol. 1, no. September 1981, pp. 68–72, 2021.

[24] A. Al-ani, A. K. Al-ani, and S. A. Laghari, “NDPsec : Neighbor Discovery Protocol Security Mechanism,” vol. 10, no. July, 2022.

[25] A. Haggag, “Implementation and Evaluation of IPv6 with Compression and Fragmentation for Throughput Improvement of Internet,” *Wirel. Pers. Commun.*, vol. 130, no. 2, pp. 1449–1477, 2023, doi: 10.1007/s11277-023-10340-4.

[26] E. M. Kwesigabo, “EVALUATING THE IMPACT OF LATENCY ON THE PERFORMANCE OF A VIRTUAL PRIVATE NETWORK USING,” vol. 4, no. 1, pp. 279–293, 2024.

[27] P. E. Kristianto and A. T. Putra, “Comparative Analysis of IPv4 and IPv6 OpenVPN Protocol Performance Based on QoS Parameters,” vol. 3, no. April, pp. 53–60, 2021.

[28] E. Kadusic, N. Zivic, C. Ruland, and N. Hadzajlic, “A Smart Parking Solution by Integrating NB-IoT Radio Communication Technology into the Core IoT Platform,” 2022.

[29] M. Shehab, “Evaluating the Effectiveness of Stealth Protocols and Proxying in Hiding VPN Usage,” vol. 4, no. August 2024, pp. 186–194, 2025, doi: 10.47852/bonviewJCCE42023642.

[30] X. Lu, M. Zhang, and L. Xu, “A survey of the cryptography enhancement technology in 5G and evolving network,” in *Proc.SPIE*, Jul. 2024, p. 131850M. doi: 10.1117/12.3033284.