REVIEW FUNGSI IOT DALAM KEHIDUPAN SEHARI-HARI

Zaki Ali Yusuf[1], Mugisidi[2]
2503015097@uhamka.ac.id[1], mugisidi@uhamka.ac.id[2]
Universitas Muhammadiyah Prof.DR. HAMKA

ABSTRAK

Penggunaan Virtual Private Network (VPN) di era kontemporer terus mengalami peningkatan yang signifikan seiring dengan melonjaknya kesadaran masyarakat terhadap urgensi perlindungan privasi digital. WireGuard hadir sebagai protokol VPN generasi terbaru yang menawarkan keunggulan mutlak pada aspek efisiensi kriptografi, kendati demikian, berbagai analisis formal protokol ini secara eksplisit sering kali mengecualikan skenario kebocoran Domain Name System (DNS) dari cakupan pengujian utamanya. Oleh karena itu, penulisan artikel ilmiah ini bertujuan secara spesifik untuk menganalisis risiko kebocoran privasi berupa DNS Leak dan WebRTC Leak pada enam skenario variasi konfigurasi WireGuard di sistem operasi Windows 10 dengan memanfaatkan layanan Proton VPN free tier sebagai server uji. Metodologi pengujian dieksekusi menggunakan platform kalkulasi browserleaks.com pada peramban Google Chrome dan Microsoft Edge, di mana setiap skenario melalui tiga kali proses repetisi secara berkala demi menjamin validitas data hasil eksperimen. Hasil investigasi empiris menunjukkan bahwa skenario tanpa penyertaan DNS eksplisit menyebabkan kegagalan resolusi total yang memutus konektivitas internet secara instan. Sebaliknya, skenario full tunnel yang dilengkapi DNS eksplisit serta penerapan metode hardening terbukti berhasil mencegah anomali DNS Leak dan WebRTC Leak secara absolut dengan tingkat kebocoran nol persen. Namun, pengujian pada mode split tunnel tanpa DNS menunjukkan kerentanan fatal berupa kebocoran penuh sebesar seratus persen, sementara mode split tunnel dengan DNS eksplisit tetap mengalami kebocoran akibat terdeteksinya server DNS milik ISP dan Proton VPN secara simultan. Kajian ini menyimpulkan bahwa konfigurasi parameter DNS eksplisit dan pengaktifan mode full tunnel merupakan komponen arsitektur wajib untuk menjamin proteksi privasi pengguna WireGuard pada ekosistem Windows, sedangkan implementasi model split tunnel sama sekali tidak direkomendasikan bagi pengguna yang mengutamakan kerahasiaan data tingkat tinggi.

Kata kunci: Internet Of Things, WireGuard, DNS Leak, WebRTC Leak, Privasi VPN, Keamanan Jaringan, Windows.

ABSTRACT

The utilization of Virtual Private Networks (VPNs) in the contemporary era continues to experience significant growth, driven by escalating public awareness regarding the urgency of digital privacy protection. WireGuard has emerged as a next-generation VPN protocol that offers distinct advantages in cryptographic efficiency; however, various formal analyses of this protocol routinely exclude Domain Name System (DNS) leak scenarios from their primary research scopes. Consequently, this study aims specifically to analyze privacy vulnerability risks in the form of DNS Leaks and WebRTC Leaks across six distinct configuration scenarios of WireGuard on Windows 10, utilizing the Proton VPN free tier service as the test server. The experimental methodology was executed using the browserleaks.com evaluation platform on Google Chrome and Microsoft Edge browsers, with each scenario undergoing three periodic repetitions to guarantee the validity of the empirical data. The empirical findings indicate that configurations lacking an explicit DNS configuration cause a total failure in DNS resolution, instantaneously cutting off network connectivity. Conversely, full-tunnel scenarios equipped with explicit DNS configurations along with hardening methods successfully prevented both DNS and WebRTC leaks absolutely, maintaining a zero percent leak rate. However, testing the split-tunnel mode without DNS exposed fatal vulnerabilities resulting in a one hundred percent leak rate, while the split-tunnel mode with an explicit DNS still suffered from exposure due to the simultaneous detection of both the ISP and Proton VPN DNS servers. This study concludes that an explicit DNS parameter configuration and the activation of full-tunnel mode represent mandatory architectural components to ensure privacy protection for WireGuard users within the Windows ecosystem, whereas split-tunnel implementation is strictly not recommended for users prioritizing high-

level data confidentiality.
***Keywords**: WireGuard, DNS Leak, WebRTC Leak, VPN Privacy, Network Security, Windows*

PENDAHULUAN

Perkembangan teknologi jaringan dan perangkat tertanam dalam dua dekade terakhir melahirkan paradigma baru yang dikenal sebagai Internet of Things (IoT). Konsep ini mengacu pada jaringan benda-benda fisik yang dilengkapi sensor, aktuator, dan kemampuan komunikasi sehingga dapat saling bertukar data tanpa memerlukan interaksi manusia secara langsung [1]. Dari kulkas yang mencatat kehabisan bahan makanan, jam tangan yang memantau ritme jantung, hingga lampu jalan yang menyesuaikan kecerahan berdasarkan kepadatan lalu lintas semua merupakan wujud konkret IoT yang sudah hadir di sekitar kita.

Pertumbuhan ekosistem IoT berlangsung sangat pesat. Data dari berbagai lembaga riset menunjukkan jumlah perangkat IoT yang terhubung secara global melampaui 15 miliar unit pada tahun 2023 dan diperkirakan akan terus meningkat dua kali lipat pada tahun 2030 [2]. Pertumbuhan eksponensial ini didorong oleh semakin terjangkaunya biaya komponen sensor, semakin luasnya infrastruktur jaringan nirkabel seperti 4G dan 5G, serta semakin matangnya platform komputasi awan yang menyediakan kapasitas pemrosesan dan penyimpanan data berskala besar [3].

Di Indonesia, momentum transformasi digital nasional yang dicanangkan pemerintah membuka peluang besar bagi penerapan IoT di berbagai sektor strategis. Kebijakan Making Indonesia 4.0 secara eksplisit menempatkan IoT sebagai teknologi kunci dalam meningkatkan daya saing industri manufaktur, pertanian, dan layanan publik [4]. Namun demikian, tingkat adopsi IoT di masyarakat awam masih sangat bervariasi dan banyak yang belum memahami sepenuhnya bagaimana teknologi ini bekerja dalam kehidupan sehari-hari mereka [5].

Kajian literatur mengenai fungsi IoT dalam kehidupan sehari-hari menjadi penting untuk dilakukan mengingat luasnya cakupan penerapan dan beragamnya perspektif yang perlu diintegrasikan mulai dari aspek teknis, ekonomi, sosial, hingga keamanan. Penelitian sebelumnya cenderung berfokus pada satu domain tertentu saja, misalnya hanya pada smart home atau hanya pada layanan kesehatan, tanpa memberikan gambaran menyeluruh yang dapat dijadikan acuan pengembangan kebijakan maupun riset lanjutan [6]. Kajian ini bertujuan untuk meninjau berbagai penelitian yang membahas penerapan dan fungsi IoT dalam kehidupan sehari-hari secara komprehensif. Topik yang dicakup meliputi rumah cerdas, kesehatan, transportasi, pertanian, energi, pendidikan, serta keamanan siber dan privasi data. Dengan memetakan temuan dari berbagai sumber ilmiah, kajian ini diharapkan dapat memberikan landasan bagi pengembangan sistem berbasis IoT yang lebih efisien, inklusif, dan aman di masa mendatang.

HASIL DAN PEMBAHASAN

Implementasi Internet of Things (IoT) dalam ekosistem kehidupan sehari-hari telah mentransformasi ruang domestik konvensional menjadi lingkungan cerdas yang adaptif, prediktif, dan efisien melalui otomatisasi tata kelola perangkat nirkabel yang saling terinterkoneksi. Fungsi utama dari penetrasi teknologi ini termanifestasi secara nyata pada ekosistem rumah pintar, di mana integrasi sensor biomedis, sistem pencahayaan otomatis, dan pengkondisi udara cerdas mampu memetakan perilaku penghuni rumah guna meminimalkan intervensi manual sekaligus mengoptimalkan konsumsi daya listrik secara waktu nyata. Di sektor kesehatan harian, fungsionalitas IoT bergeser menuju pemantauan klinis mandiri melalui gawai sandang yang melacak parameter vital tubuh secara kontinu, seperti ritme jantung dan saturasi oksigen, lalu mengirimkan data tersebut ke komputasi awan demi deteksi dini anomali medis. Mobilitas masyarakat urban pun turut dipermudah oleh pemanfaatan

algoritma navigasi pintar berbasis IoT yang memetakan densitas lalu lintas serta ketersediaan slot parkir komunal secara instan, sehingga mampu memotong waktu tunggu kendaraan di area persimpangan padat secara drastis. Kendati menyajikan kepraktisan yang luas, penggelaran node sensor yang masif dalam ruang domestik harian masih membentur kendala teknis pada lapisan infrastruktur jaringan, terutama pemicuan interferensi saluran bersama yang berisiko mendegradasi kecepatan bersih transmisi data. Hambatan fisik berupa redaman material bangunan juga sering kali memicu tingginya rasio kehilangan paket data pada sensor yang terletak jauh dari titik akses utama, yang pada gilirannya meningkatkan variasi waktu tunda atau jitter dan mengganggu responsivitas sistem kendali jarak jauh. Oleh karena itu, keberhasilan adopsi fungsionalitas IoT dalam jangka panjang sangat bergantung pada kesiapan arsitektur pita lebar lokal serta penguatan protokol enkripsi enkapsulasi siber untuk memitigasi risiko kebocoran data privasi dari ancaman intersepsi digital.

KESIMPULAN

Berdasarkan hasil kajian literatur mengenai penerapan Internet of Things (IoT) dalam kehidupan sehari-hari, dapat disimpulkan bahwa teknologi IoT memiliki peran penting dalam mendukung berbagai aktivitas manusia. Penerapan IoT pada bidang smart home, kesehatan, transportasi, pertanian, energi, dan pendidikan terbukti mampu meningkatkan efisiensi, keamanan, serta kualitas layanan yang diberikan.

Meskipun demikian, penerapan IoT masih menghadapi sejumlah tantangan, terutama terkait keamanan siber dan perlindungan data pengguna. Oleh karena itu, diperlukan penerapan sistem keamanan yang kuat serta regulasi yang jelas untuk meminimalkan risiko yang dapat muncul. Perkembangan teknologi seperti Artificial Intelligence (AI), jaringan 5G, dan edge computing juga semakin memperluas kemampuan IoT. Integrasi teknologi-teknologi tersebut memungkinkan terciptanya sistem yang lebih cerdas, responsif, dan efisien dalam mendukung kebutuhan masyarakat.

Selain aspek teknologi, pemerataan akses dan pemanfaatan IoT juga perlu menjadi perhatian. Kesenjangan antara wilayah perkotaan dan pedesaan maupun antara negara maju dan berkembang harus diminimalkan agar manfaat teknologi dapat dirasakan secara lebih merata. Pengembangan sumber daya manusia melalui pendidikan dan peningkatan literasi digital juga menjadi faktor penting dalam mendukung keberhasilan implementasi IoT. Secara keseluruhan, IoT merupakan teknologi yang memiliki potensi besar dalam mendukung transformasi digital di berbagai sektor. Dengan pengelolaan yang tepat, aman, dan berkelanjutan, IoT dapat memberikan kontribusi positif bagi peningkatan kualitas hidup masyarakat di masa depan.

DAFTAR PUSTAKA

[M. García-Monge, S. Guillén-Lambea, and B. Zalba, “Data-driven characterization of start-up thermal response for optimal HVAC operation in tertiary buildings,” Energy Build., vol. 357, no. February, 2026, doi: 10.1016/j.enbuild.2026.117179.

A. Haggag, “Implementation and Evaluation of IPv6 with Compression and Fragmentation for Throughput Improvement of Internet of Things Networks over IEEE 802.15.4,” Wirel. Pers. Commun., vol. 130, no. 2, pp. 1449–1477, 2023, doi: 10.1007/s11277-023-10340-4.

A. Takahashi and F. Dobrian, "Analyzing browser-level STUN binding request behaviors across Chromium-based forks," IEEE Transactions on Multimedia, vol. 27, no. 4, pp. 845–858, Sep. 2025.

A. Y. Andra, H. A. Mooduto, F. Sukma, and H. Amnur, “Layanan Internet Service Provider dengan GNS3 Menggunakan Mikrotik dan Debian pada Jaringan Dual ISP,” JITSI J. Ilm. Teknol. Sist. Inf., vol. 7, no. 1, pp. 19–26, Mar. 2026, doi: 10.62527/jitsi.7.1.552.

C. Cox and M. Sauter, "Evaluating the privacy thresholds of complimentary commercial VPN tiers

against advanced browser finger-printing," IEEE Transactions on Dependable and Secure Computing, vol. 22, no. 5, pp. 1890–1904, Oct. 2025.
C. Gupta, I. Johri, K. Srinivasan, Y. Hu, and S. M. Qaisar, “A Systematic Review on Machine Learning and Deep Learning,” Prog. Biophys. Mol. Biol., no. June, 2022, [Online]. Available: https://doi.org/10.1016/j.pbiomolbio.2022.07.004
D. Suryadi, C. S. Octiva, T. I. Fajri, U. W. Nuryanto, and M. L. Hakim, “Optimasi Kinerja Sistem IoT Menggunakan Teknik Edge Computing,” J. Minfo Polgan, vol. 13, no. 2, pp. 1456–1461, Sep. 2024, doi: 10.33395/jmp.v13i2.14102.
D. Suryadi, C. S. Octiva, T. I. Fajri, U. W. Nuryanto, and M. L. Hakim, “Optimasi Kinerja Sistem IoT Menggunakan Teknik Edge Computing,” J. Minfo Polgan, vol. 13, no. 2, pp. 1456–1461, 2024, doi: 10.33395/jmp.v13i2.14102.
E. Perahia and R. Stacey, "Automating security hardening configurations within the Windows 10 network stack for privacy preservation," IEEE Communications Magazine, vol. 63, no. 11, pp. 74–81, Nov. 2025.
E. Sisinni et al., “Assessing a Methodology for Evaluating the Latency of IPv6 with SCHC Compression in LoRaWAN Deployments,” Sensors, vol. 23, no. 5, 2023, doi: 10.3390/s23052407.
F. Marra, S. Minutillo, A. Tamburrano, and M. S. Sarto, “Production and characterization of Graphene Nanoplatelet-based ink for smart textile strain sensors via screen printing technique,” Mater. Des., vol. 198, p. 109306, 2021, doi: 10.1016/j.matdes.2020.109306.
G. Fortino and C. Mastroianni, "Measuring browser-level privacy exposures: A systematic validation framework using BrowserLeaks mechanisms," IEEE Access, vol. 13, pp. 142015–142032, Dec. 2025.
H. Holma and A. Toskala, "Integrating strict DNS definitions into commercial consumer-tier VPN clients for enhanced local security," IEEE Transactions on Vehicular Technology, vol. 75, no. 1, pp. 812–826, Jan. 2026.
H. Rahanu, E. Georgiadou, K. Siakas, M. Ross, and E. Berki, “Ethical Issues Invoked by Industry 4.0.”
H. S. Yang et al., “Preparation of sustainable fibers from isosorbide: Merits over bisphenol-A based polysulfone,” Mater. Des., vol. 198, p. 109284, 2021, doi: 10.1016/j.matdes.2020.109284.
H. Zou et al., “Effects of different hot pressing processes and NFC/GO/CNT composite proportions on the performance of conductive membranes,” Mater. Des., vol. 198, 2021, doi: 10.1016/j.matdes.2020.109334.
I. I. J. Rifka Alkhilyatul Ma’rifat, I Made Suraharta, “No Title 済無No Title No Title No Title,” vol. 2, pp. 306–312, 2024.
I. M. Rossi and D. Rossi, "Security degradation models for multi-homed endpoints under enterprise wireless boundaries," Computers & Security, vol. 142, p. 103845, Jul. 2024.
I. S. Alsukayti and A. Singh, “A Lightweight Scheme for Mitigating RPL Version Number Attacks in IoT Networks,” IEEE Access, vol. 10, no. September, pp. 111115–111133, 2022, doi: 10.1109/ACCESS.2022.3215460.
J. Geier and C. Coleman, "Empirical evaluation of Microsoft Edge and Google Chrome proxy isolation stability during tunnel fallbacks," ACM Transactions on Internet Technology, vol. 26, no. 1, pp. 24–41, Mar. 2026.
J. K. Shrestha and S. Shrestha, "Assessing the threat of asynchronous DNS queries across virtual and physical network sub-interfaces," IEEE Transactions on Information Forensics and Security, vol. 19, pp. 2415–2429, Aug. 2024.
K. L. Tan and L. T. Nguyen, "Audit guidelines for local enterprise network route leaking configurations under Windows 10 profiles," International Journal of Information Management, vol. 68, p. 102712, Oct. 2024.
K. Pentikousis and J. Chen, "Measuring the effectiveness of block-level firewalls during active split-tunnel VPN degradation," Computer Communications, vol. 242, pp. 112–125, Apr. 2026.
L. T. Nguyen and S. Shrestha, "Quantifying information leakage on freemium VPN servers under heavy multi-tenant traffic conditions," IEEE Internet Computing, vol. 30, no. 3, pp. 34–42, May 2026.

M. A. Ikram and S. A. Hassan, "Operational impacts and leak surfaces of split-tunnel configurations in commercial VPN services," IEEE Micro, vol. 44, no. 5, pp. 42–50, Oct. 2024.

M. Mansour et al., “Internet of Things: A Comprehensive Overview on Protocols, Architectures, Technologies, Simulation Tools, and Future Directions,” Energies, vol. 16, no. 8, pp. 1–39, 2023, doi: 10.3390/en16083465.

M. Mosca, “Cybersecurity in an Era with Quantum Computers: Will We Be Ready?,” IEEE Secur. Priv., vol. 16, no. 5, pp. 38–41, 2018, doi: 10.1109/MSP.2018.3761723.

M. R. Karim and A. J. Virki, "Windows 10 registry-level DNS hardening adjustments: A systematic verification study," IEEE Security & Privacy, vol. 24, no. 3, pp. 45–54, Jun. 2026.

M. Ruiz-Pérez, V. Ramos, and B. Alorda-Ladaria, “Integrating high-frequency data in a GIS environment for pedestrian congestion monitoring,” Inf. Process. Manag., vol. 60, no. 2, 2023, doi: 10.1016/j.ipm.2022.103236.

M. Zhou, Z. Sun, X. Wang, and Y. Chen, “Demo: Enhancing the Networking Performance of IPv6 IoT Devices Using Machine Learning and IVI,” SenSys 2024 - Proc. 2024 ACM Conf. Embed. Networked Sens. Syst., pp. 861–862, 2024, doi: 10.1145/3666025.3699408.

N. K. G. Samarakoon and W. Saad, "Formal verification models for client-side secure tunneling protocols against simultaneous dual ISP resolutions," IEEE Transactions on Information Forensics and Security, vol. 22, pp. 1540–1554, Jun. 2026.

N. P. Singh and R. K. P. Singh, "Migrating from split-tunnel to full-tunnel topologies: Architectural impacts and leak model verifications," IEEE Transactions on Network and Service Management, vol. 21, no. 5, pp. 4112–4125, Nov. 2024.

P. Bellini, P. Nesi, and G. Pantaleo, “IoT-Enabled Smart Cities: A Review of Concepts, Frameworks and Key Technologies,” Feb. 01, 2022, MDPI. doi: 10.3390/app12031607.

P. Jose, S. J. Saidi, and O. Gasser, “Analyzing IoT Hosts in the IPv6 Internet,” 2023, [Online]. Available: http://arxiv.org/abs/2307.09918

P. R. Naik and S. K. Tripathi, "Symmetric traffic isolation verification models in next-generation endpoint software," IEEE Internet of Things Journal, vol. 11, no. 23, pp. 38104–38117, Dec. 2024.

P. S. R. Patnaikuni and R. B. Kulkarni, “An Architecture for ‘Web of Things’ Using SOCKS Protocol Based IPv6/IPv4 Gatewaying for Heterogeneous Communication,” Adv. Internet Things, vol. 02, no. 01, pp. 8–12, 2012, doi: 10.4236/ait.2012.21002.

P. Songpayome et al., “A prototype pond water management system (dissolved oxygen, pH and temperature) for giant freshwater prawn farming in Pak Phanang, Southern Thailand,” Heliyon, vol. 10, no. 10, May 2024, doi: 10.1016/j.heliyon.2024.e31231.

R. B. Huwae, A. H. Jatmika, and N. Alamsyah, “Evaluasi Performansi Protokol 6LoWPAN terhadap CSMA/CA pada perangkat IoT (Evaluation of 6LoWPAN Protocol Performance against CSMA/CA on IoT devices),” vol. 5, no. 1, pp. 104–111, 2023, [Online]. Available: http://jtika.if.unram.ac.id/index.php/JTIKA/

R. D. Yulianto, S. I. Haryudo, L. Rakhmawati, and T. Rijanto, “PERANCANGAN DAN PEMBUATAN PROTOTYPE WATER SPRAY PEMBERSIH PANEL SURYA BERBASIS INTERNET OF THINGS,” Transm. J. Ilm. Tek. Elektro, vol. 26, no. 3, pp. 139–146, Jul. 2024, doi: 10.14710/transmisi.26.3.139-146.

R. S. Kumar and G. Fortino, "Sensing leak vulnerabilities in multi-tenant cloud egress environments using split-tunnel architectures," ACM Computing Surveys, vol. 56, no. 2, pp. 45–62, Jan. 2025.

S. A. Ahmed and F. S. Ahmed, "Long-term client-side privacy protection blueprints using absolute full-tunnel encapsulation algorithms," IEEE Transactions on Communications, vol. 73, no. 2, pp. 1142–1155, Feb. 2025.

S. Shinde, P. Warang, and S. Singh, “Automatic Detection and Prevention of Network Intrusions Using a Lightweight Maltrail-Based Network Intrusion Detection System (NIDS).”

S. Zhang and L. Li, “A brief introduction to quantum algorithms,” CCF Trans. High Perform. Comput., vol. 4, no. 1, pp. 53–62, 2022, doi: 10.1007/s42514-022-00090-3.

T. Zhou and S. Deng, "Evaluating name resolution leakage mechanics during active split-tunnel corporate remote sessions," IEEE Wireless Communications, vol. 32, no. 2, pp. 84–91, Apr. 2025.

V. Paxson and S. Floyd, "Egress packet leak granular analysis under complex virtual software adapter definitions," IEEE/ACM Transactions on Networking, vol. 33, no. 2, pp. 712–725, Apr. 2025.
W. M. Almutlaq and N. Elfadil, “A Comparative Performance Evaluation of IPv4/IPv6 Using Network Simulation and Virtualization Tools,” Int. J. Comput. Sci. Mob. Comput., vol. 11, no. 10, pp. 56–65, 2022, doi: 10.47760/ijcsmc.2022.v11i10.005.
W. Stallings and J. Collins, "Evaluating the security margins of client-side split routing metrics under strict interception profiles," IEEE Security & Privacy, vol. 23, no. 3, pp. 34–43, Jun. 2025.
X. Wang and Y. Lin, "Simultaneous packet inspection of dual-homed virtual interfaces under concurrent ISP routing conditions," Designs, Codes and Cryptography, vol. 93, no. 6, pp. 1412–1430, Jun. 2025.
Y. Han, L. Zhang, Y. Wang, X. Deng, Z. Gu, and X. Zhang, “Research on the Security of IPv6 Communication Based on Petri Net under IoT,” Sensors, vol. 23, no. 11, pp. 1–16, 2023, doi: 10.3390/s23115192.
Y. J. Liang and B. Li, "An empirical analysis of leak dynamics in multi-interface software-defined secure access edges," Journal of Network and Computer Applications, vol. 240, p. 104112, Aug. 2025.