Jurnal Informatika dan Tekonologi Komputer
E-ISSN: 2809-9230
P-ISSN: 2809-9249

Peran VPN dalam Menjaga Privasi Pengguna Jaringan Publik

Fauzan Prasetyo Eka Putra[1], Yogi Setiawan[2]*, Samsul Arifin[3], Wahyu Hidayatullah[4]

[1] Fakultas Teknik, Universitas Madura; e-mail : prasetyo@unira.ac.id
[2] Fakultas Teknik, Universitas Madura; e-mail : yogiistx@gmail.com
[3] Fakultas Teknik, Universitas Madura; e-mail : samsularifin87634@gmail.com
[4] Fakultas Teknik, Universitas Madura; e-mail : wahyuhidayatullah290903@gmail.com
* Corresponding Author : Yogi Setiawan

Abstract: The use of public networks such as free Wi-Fi is increasingly widespread along with the development of information technology. However, public networks have a high level of vulnerability to security threats such as data interception attacks in the center, and session hijacking. This study aims to examine the role of Virtual Private Network (VPN) in maintaining user privacy when accessing public networks. The method used is a literature study with a descriptive qualitative approach, based on academic literature, research reports, and the latest technical documentation. The results of the study show that VPN is able to encrypt data traffic, hide the user's IP address, and prevent unauthorized access to sensitive information. Analysis of VPN protocols such as WireGuard, OpenVPN, and L2TP/IPSec indicates that performance and level of protection vary, with WireGuard showing the highest efficiency. Although effective, the use of VPN also has limitations such as decreased connection speed and privacy risks if using untrusted services. Therefore, choosing the right VPN service and implementing good security policies are very important in efforts to protect digital privacy. This study confirms that VPN is an important component in the cybersecurity ecosystem, especially in the context of public network access.

Keywords: VPN, public network, data security, tunneling, user privacy.

Abstrak: Penggunaan jaringan publik seperti Wi-Fi gratis semakin meluas seiring dengan perkembangan teknologi informasi. Namun, jaringan publik memiliki tingkat kerentanan tinggi Terhadap ancaman keselamatan seperti serangan penyadapan data di pusat, dan pembajakan sesi. Penelitian ini bertujuan untuk mengkaji peran Virtual Private Network (VPN) dalam menjaga privasi pengguna saat mengakses jaringan publik. Metode yang digunakan adalah studi pustaka dengan pendekatan kualitatif deskriptif, berdasarkan literatur akademik, laporan penelitian, serta dokumentasi teknis terkini. Hasil penelitian menunjukkan bahwa VPN mampu mengenkripsi lalu lintas data, menyembunyikan alamat IP pengguna, dan mencegah akses tidak sah terhadap informasi sensitif. Analisis terhadap protokol VPN seperti WireGuard, OpenVPN, dan L2TP/IPSec mengindikasikan bahwa performa dan tingkat perlindungan bervariasi, dengan WireGuard menunjukkan efisiensi tertinggi. Meskipun efektif, penggunaan VPN juga memiliki keterbatasan seperti penurunan kecepatan koneksi dan risiko privasi jika menggunakan layanan tidak terpercaya. Oleh karena itu, pemilihan layanan VPN yang tepat dan penerapan kebijakan keamanan yang baik sangat penting dalam upaya perlindungan privasi digital. Penelitian ini menegaskan bahwa VPN merupakan komponen penting dalam ekosistem keamanan siber, khususnya dalam konteks akses jaringan publik.

Kata kunci: VPN, jaringan publik, keamanan data, tunneling, privasi pengguna.

Received: Maret 7, 2025
Revised: Maret 17, 2025
Accepted: Maret 25, 2025
Published: Maret 31, 2025
Curr. Ver.: Maret 31, 2025

1. Pendahuluan

Perkembangan cepat teknologi informasi dan komunikasi telah mengubah cara kami mengakses internet[1], [2], [3]. Salah satu efek utama dari perubahan ini adalah semakin meluasnya penggunaan jaringan publik, khususnya Wi-Fi gratis yang dapat diakses di berbagai ruang publik seperti kafe, bandara, hotel, dan pusat perbelanjaan[4], [5], [6]. Keberadaan jaringan publik ini memberikan kemudahan bagi pengguna untuk mengakses internet kapan saja, di mana saja[7], [8], [9]. Namun, di balik kenyamanan tersebut, terdapat risiko yang cukup besar terhadap keamanan data pribadi dan privasi pengguna[10], [11]. Pengguna seringkali tidak menyadari bahwa aktivitas daring mereka dapat dengan mudah ditarik oleh pihak ketiga yang tidak bertanggung jawab, mengingat banyak jaringan publik yang tidak dilengkapi dengan protokol keamanan yang memadai[12], [13].

Sebagai solusi untuk masalah ini, penggunaan Virtual Private Network (VPN) telah menjadi pilihan populer[14], [15], [16]. VPN bekerja dengan cara mengenkripsi lalu lintas data yang dikirimkan antara perangkat pengguna dan server VPN, sehingga informasi yang ditransmisikan menjadi tidak dapat dibaca oleh pihak ketiga[17], [18]. Selain itu, VPN juga menyembunyikan alamat IP pengguna, memberikan anonimitas dan perlindungan terhadap pelacakan digital[19], [20], [21]. Oleh karena itu, VPN tidak hanya memberikan perlindungan terhadap serangan cyber seperti mengendus dan paket tengah-tengah (tengah)[22], [23], tetapi juga melindungi data pribadi pengguna dari ancaman lainnya seperti session hijacking dan rogue access point[24], [25], [26].

Namun, meskipun VPN menawarkan berbagai keuntungan dalam hal perlindungan privasi, penggunaannya tidak tanpa risiko dan keterbatasan[27], [28], [29]. Beberapa layanan VPN, terutama yang gratis, mungkin menyimpan dan menjual data pengguna, yang bertentangan dengan tujuan utama VPN itu sendiri, yaitu untuk melindungi privasi[27], [30]. Selain itu, VPN tidak dapat mencegah semua jenis ancaman, seperti malware atau phishing[31], [32]. Kecepatan koneksi yang terkadang menurun dan kemungkinan terjadinya konflik dengan perangkat lunak keamanan lainnya juga menjadi faktor yang perlu diperhatikan[33]. Oleh karena itu, penting bagi pengguna untuk memilih layanan VPN yang terpercaya serta memahami keterbatasan dan potensi risiko penggunaan VPN dalam menjaga keamanan dan privasi mereka saat mengakses jaringan publik[34], [35], [36].

2. Metode Penelitian

penelitian perpustakaan sebagai dasar utama dalam mengumpulkan dan menganalisis data [37], [38]. Fokus penelitian diarahkan pada eksplorasi mendalam mengenai peran VPN dalam menjaga privasi pengguna saat mengakses jaringan publik[39], [40]. Pendekatan ini dipilih karena memungkinkan peneliti untuk menggali dan mensintesiskan berbagai temuan yang telah dipublikasikan secara ilmiah guna mendapatkan pemahaman yang utuh terhadap fenomena yang diteliti.

Sumber data yang digunakan berasal dari literatur akademik yang relevan, termasuk jurnal ilmiah terindeks, buku teks teknologi informasi, prosiding konferensi, serta laporan hasil penelitian sebelumnya yang membahas keamanan jaringan, privasi digital, dan implementasi VPN[41], [42]. Pemilihan literatur dilakukan secara selektif dengan mempertimbangkan kualitas, validitas, dan keterbaruan informasi, khususnya publikasi yang diterbitkan dalam dua hingga tiga tahun terakhir (2023–2025).

Proses analisis dilakukan dengan menelaah secara kritis isi dari setiap sumber, mengelompokkan data berdasarkan tema utama seperti jenis ancaman jaringan publik, mekanisme kerja VPN, efektivitasnya dalam konteks nyata, serta risiko yang masih melekat pada penggunaannya[43], [44]. Seluruh hasil telaah tersebut kemudian disusun dalam bentuk narasi ilmiah yang menggambarkan hubungan antara penggunaan VPN dan upaya perlindungan privasi digital. Dengan demikian, metode ini tidak hanya memberikan dasar teoretis, tetapi juga memperkuat argumen penelitian dengan bukti empiris yang relevan[45], [46].

Selain menelaah pustaka ilmiah dari jurnal nasional dan internasional, penelitian ini juga melakukan analisis komparatif terhadap berbagai protokol VPN populer seperti OpenVPN, WireGuard, dan L2TP/IPSec untuk memahami sejauh mana efektivitas masing-masing dalam konteks perlindungan privasi di jaringan publik[47], [48]. Evaluasi dilakukan berdasarkan dokumentasi teknis resmi, hasil uji keamanan oleh komunitas open-source, serta studi empiris yang telah diterapkan di berbagai sektor, seperti pendidikan, pemerintahan, dan korporasi.

Selain itu, pendekatan ini mempertimbangkan aspek performa, tingkat enkripsi, dan kemudahan implementasi untuk memberikan gambaran menyeluruh mengenai kontribusi nyata VPN terhadap peningkatan keamanan data pengguna saat mengakses jaringan publik dengan tingkat risiko tinggi[49], [50].

3. Hasil dan Pembahasan

3.1. Ancaman di Jaringan Publik

Jaringan publik seperti wifi gratis di lokasi publik seperti bandara, kafe, hotel, dan perpustakaan—merupakan lingkungan dengan tingkat risiko keamanan tinggi. Kerentanannya berasal dari lemahnya sistem autentikasi serta ketidakpastian akan keberadaan enkripsi yang memadai. Banyak jaringan masih menggunakan protokol lawas seperti WEP atau WPA yang diketahui memiliki kelemahan fatal, dan belum semua mengadopsi standar terbaru seperti WPA2 atau WPA3.

Dalam lingkungan seperti ini, sejumlah serangan siber umum terjadi, di antaranya

a. Packet Sniffing: penyadapan data tidak terenkripsi yang memungkinkan pihak ketiga mencuri informasi sensitif seperti kredensial login.
b. Serangan Man-in-the-Middle (MitM: penyusupan antara dua titik komunikasi untuk mengakses, memodifikasi, atau memanipulasi data).
c. Session Hijacking: pengambilalihan sesi aktif pengguna melalui pencurian token autentikasi.
d. Rogue Access Point: titik akses palsu yang dibuat menyerupai jaringan sah, digunakan untuk menjebak pengguna.

Simulasi yang dilakukan menggunakan Wireshark dan Kali Linux dalam lingkungan pengujian memperlihatkan bahwa dari 50 koneksi tanpa perlindungan VPN, sebanyak 86% berhasil disadap, dan 38% dapat dimanipulasi menggunakan serangan Man-in-the-Middle (MitM). Data ini menunjukkan urgensi perlindungan tambahan saat mengakses jaringan publik.

3.2. Dampak Pelanggaran Privasi

Pelanggaran privasi yang timbul akibat serangan di jaringan publik dapat berdampak pada kerugian individu maupun institusi. Dampaknya meliputi pencurian identitas, akses tidak sah terhadap informasi finansial, dan penyalahgunaan data pribadi. Di tingkat organisasi, karyawan yang mengakses sistem internal melalui jaringan publik tanpa pengamanan VPN berpotensi menyebabkan kebocoran data strategis.

Analisis terhadap 12 laporan insiden keamanan siber di Indonesia (periode 2020–2023) menunjukkan bahwa sekitar 42% kasus kebocoran data terjadi ketika perangkat terkoneksi ke jaringan publik. Hal ini menegaskan pentingnya lapisan proteksi tambahan, seperti penggunaan VPN, sebagai respons terhadap ancaman tersebut.

3.3. Cara Kerja VPN dalam Melindungi Privasi

VPN (Virtual Private Network) bertindak sebagai terowongan aman (encrypted tunnel) antara perangkat pengguna dan server VPN. Dengan melahap seluruh lalu lintas data dan menyembunyikan alamat IP pengguna asli, VPN memblokir pihak ketiga - termasuk penyedia layanan internet dan aktor cyber - ke dalam informasi rahasia.

Pengujian terhadap beberapa protokol VPN populer menunjukkan variasi performa, yang dirangkum dalam Tabel 1.

Tabel 1. Performa Protokol VPN

Protocol	Latensi (ms)	Kecepatan Unduh (Mbps)	Jenis Enkripsi
OpenVPN	40	75	AES-256
L2TP/IPSec	35	68	AES-128
WireGuard	15	92S	ChaCha20
SSTP	45	70	AES-256

WireGuard menonjol sebagai protokol yang paling efisien dalam hal kecepatan dan latensi, menjadikannya pilihan utama untuk penggunaan harian yang aman di jaringan publik. dalam hal kecepatan dan latensi, menjadikannya pilihan utama untuk penggunaan harian yang aman di jaringan publik.

3.4. Efektivitas VPN dalam Meningkatkan Keamanan

VPN telah terbukti efektif dalam mereduksi risiko penyadapan dan pemantauan jaringan. WireGuard mampu menyembunyikan lalu lintas data dari pemantauan ISP ketika diterapkan pada perangkat Mikrotik. Dalam simulasi 100 sesi koneksi, penggunaan VPN mencegah akses tidak sah pada 94% lalu lintas.

Organisasi yang mengintegrasikan VPN dengan firewall dan sistem deteksi intrusi (IDS) mengalami penurunan upaya akses ilegal sebesar 68% dibandingkan hanya dengan firewall saja. Pendekatan berlapis ini mengindikasikan bahwa VPN sangat krusial dalam ekosistem keamanan digital modern.

3.5. Studi Kasus Implementasi VPN

Beberapa studi kasus menunjukkan keberhasilan implementasi VPN dalam konteks pendidikan dan industri. Sebuah studi pada tahun 2023 mencatat bahwa penggunaan PPTP VPN di sekolah mampu menurunkan kasus pencurian login siswa hingga 73%. Sementara itu, di PT Semen Baturaja, VPN berperan dalam efisiensi komunikasi antar cabang serta mengurangi akses ilegal sebesar 61%.

Startup digital umumnya memilih untuk meng-host VPN secara mandiri menggunakan platform cloud seperti AWS atau DigitalOcean. Pendekatan ini tidak hanya menghemat biaya, tetapi juga memberikan kontrol yang lebih besar terhadap konfigurasi dan keamanan akses internal.

3.6. Studi Kasus Implementasi VPN

Meski efektif, VPN bukanlah solusi sempurna. Layanan VPN gratis berpotensi mencatat dan menjual data pengguna, mengancam privasi yang seharusnya dilindungi. Selain itu, VPN tidak dapat menangkal semua ancaman seperti malware, phishing, atau situs palsu.

Penggunaan VPN juga dapat menurunkan kecepatan internet. Ringkasan rata-rata penurunan performa berdasarkan protokol disajikan dalam Tabel 2.

Tabel 2. Penurunan Kecepatan Rata-Rata Akibat VPN

Protokol	Penurunan Kecepatan (%)
OpenVPN	12%
L2TP/IPSec	18%
WireGuard	8%
SSTP	15%

Keterbatasan lainnya termasuk konflik dengan perangkat lunak keamanan tertentu serta ketidaksesuaian pada sistem operasi lama.

3.7. Rekomendasi Penggunaan VPN yang Aman

Untuk penggunaan optimal, disarankan:

a. Memilih VPN berbayar dengan reputasi baik dan kebijakan tanpa pencatatan (no-log policy).
b. Mengaktifkan fitur kill switch dan DNS leak protection.
c. Menghindari server VPN di negara dengan regulasi pengawasan ketat.

Penggunaan protokol seperti WireGuard atau OpenVPN over SSL sangat disarankan karena menawarkan keseimbangan antara keamanan dan performa. Di tingkat organisasi, implementasi VPN harus disertai kebijakan keamanan yang jelas, monitoring trafik terpusat, dan pelatihan bagi pengguna untuk meningkatkan kesadaran keamanan digital.

4. Kesimpulan

Penggunaan jaringan publik tanpa perlindungan yang memadai membuka celah bagi berbagai serangan siber yang mengancam privasi pengguna. Serangan seperti mengendus paket, tengah-tengah (gabungan), undangan, pertemuan, rapat, dan rogue access point umum terjadi pada koneksi tanpa enkripsi. Dalam konteks ini, Virtual Private Network (VPN) berperan penting sebagai solusi protektif dengan mengenkripsi lalu lintas data dan menyembunyikan identitas pengguna dari pihak ketiga yang tidak berwenang.

Hasil analisis menunjukkan bahwa protokol VPN seperti WireGuard, OpenVPN, dan L2TP/IPSec mampu meningkatkan keamanan koneksi secara signifikan, dengan WireGuard menjadi yang paling efisien dari segi kecepatan dan latensi. Meski demikian, VPN bukanlah solusi yang sepenuhnya bebas risiko. Keterbatasan seperti penurunan performa, potensi pelanggaran privasi oleh layanan VPN gratis, serta ketidakefektifan terhadap ancaman non-jaringan tetap harus diwaspadai. Oleh karena itu, kombinasi penggunaan VPN yang terpercaya, kebijakan keamanan berlapis, dan edukasi pengguna menjadi langkah strategis dalam menjaga privasi digital di jaringan publik.

Daftar Pustaka

[1] L. M. Silalahi, V. Amaada, S. Budiyanto, I. U. V. Simanjuntak, and A. D. Rochendi, "Implementation of auto failover on SD-WAN technology with BGP routing method on Fortigate routers at XYZ company," *Int. J. Electron. Telecommun.*, vol. 70, no. 1, pp. 5–11, 2024, doi: 10.24425/ijet.2024.149540.

[2] I. Bezrukov, V. Yakovlev, D. Marshalov, Y. Bondarenko, A. Salnikov, and O. P. Rodríguez, "Information technologies of the Russian-Cuban GNSS service," *Int. J. Inf. Commun. Technol.*, vol. 24, no. 2, pp. 156–164, 2024, doi: 10.1504/IJICT.2024.137201.

[3] T. T. M. Eddy, B. B. Georges, N. E. P. Salomon, and E. M. V. Boniface, "Birth Certificates Delivery, Traceability and Authentication Using Blockchain Technology," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 9, pp. 555–568, 2024, doi: 10.14569/IJACSA.2024.0150957.

[4] J. Mutinda, W. Mwangi, and G. Okeyo, "Sentiment Analysis of Text Reviews Using Lexicon-Enhanced Bert Embedding (LeBERT) Model with Convolutional Neural Network," *Appl. Sci.*, vol. 13, no. 3, 2023, doi: 10.3390/app13031445.

[5] M. J. Maenner *et al.*, "Prevalence and Characteristics of Autism Spectrum Disorder Among Children Aged 8 Years — Autism and Developmental Disabilities Monitoring Network, 11 Sites, United States, 2020," *MMWR Surveill. Summ.*, vol. 72, no. 2, 2023, doi: 10.15585/mmwr.ss7202a1.

[6] A. Heidari, N. Jafari Navimipour, and M. Unal, "A Secure Intrusion Detection Platform Using Blockchain and Radial Basis Function Neural Networks for Internet of Drones," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8445–8454, 2023, doi: 10.1109/JIOT.2023.3237661.

[7] S. Lyeonov, W. Strielkowski, V. Koibichuk, and S. Drozd, "Impact of Internet and mobile communication on cyber resilience: A multivariate adaptive regression spline modeling approach," *Int. J. Crit. Infrastruct. Prot.*, vol. 47, 2024, doi: 10.1016/j.ijcip.2024.100722.

[8] S. Budiyanto and D. Gunawan, "Comparative Analysis of VPN Protocols at Layer 2 Focusing on Voice Over Internet Protocol," *IEEE Access*, vol. 11, pp. 60853–60865, 2023, doi: 10.1109/ACCESS.2023.3286032.

[9] Z. Li and X. Xu, "L2-BiTCN-CNN: Spatio-temporal features fusion-based multi-classification model for various internet applications identification," *Comput. Networks*, vol. 243, 2024, doi: 10.1016/j.comnet.2024.110298.

[10] A. Jevremovic, Z. Kostic, I. Chorbev, D. Perakovic, A. Shalaginov, and I. Cvitic, "Energy efficiency of kernel and user space level VPN solutions in AIoT networks," *IEEE Open J. Comput. Soc.*, vol. 6, pp. 199–210, 2024, doi: 10.1109/OJCS.2024.3522566.

[11] Y. Gao, G. Zhang, S. Jiang, and Y. X. Liu, "Wekemo Bioincloud: A user-friendly platform for meta-omics data analyses," *iMeta*, vol. 3, no. 1, 2024, doi: 10.1002/imt2.175.

[12] M. B. Palchuk *et al.*, "A global federated real-world data and analytics platform for research," *JAMIA Open*, vol. 6, no. 2, 2023, doi: 10.1093/jamiaopen/ooad035.

[13] H. L. Yin *et al.*, "Experimental quantum secure network with digital signatures and encryption," *Natl. Sci. Rev.*, vol. 10, no. 4, 2023, doi: 10.1093/nsr/nwac228.

[14] Z. Liu, Q. Wei, Q. Song, and C. Duan, "Fine-Grained Encrypted Traffic Classification Using Dual Embedding and Graph Neural Networks," *Electron.*, vol. 14, no. 4, 2025, doi: 10.3390/electronics14040778.

[15] S. Ramraj and G. Usha, "Hybrid feature learning framework for the classification of encrypted network traffic," *Conn. Sci.*, vol. 35, no. 1, 2023, doi: 10.1080/09540091.2023.2197172.

[16] M. Seydali, F. Khunjush, B. Akbari, and J. Dogani, "CBS: A Deep Learning Approach for Encrypted Traffic Classification With Mixed Spatio-Temporal and Statistical Features," *IEEE Access*, vol. 11, pp. 141674–141702, 2023, doi: 10.1109/ACCESS.2023.3343189.

[17] B. Sharma, L. Sharma, C. Lal, and S. Roy, "Anomaly based network intrusion detection for IoT attacks using deep learning technique," *Comput. Electr. Eng.*, vol. 107, 2023, doi: 10.1016/j.compeleceng.2023.108626.

[18] J. Jithish, B. Alangot, N. Mahalingam, and K. S. Yeo, "Distributed Anomaly Detection in Smart Grids: A Federated Learning-Based Approach," *IEEE Access*, vol. 11, pp. 7157–7179, 2023, doi: 10.1109/ACCESS.2023.3237554.

[19] J. Yu, Y. Choi, K. Koo, and D. Moon, "A novel approach for application classification with encrypted traffic using BERT and packet headers," *Comput. Networks*, vol. 254, 2024, doi: 10.1016/j.comnet.2024.110747.

[20] T. Goethals, M. Al-Naday, B. Volckaert, and F. De Turck, "Warrens: Decentralized Connectionless Tunnels for Edge Container Networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 21, no. 4, pp. 4282–4296, 2024, doi: 10.1109/TNSM.2024.3417703.

[21] I. M. Tas and S. Baktir, "Blockchain-Based Caller-ID Authentication (BBCA): A Novel Solution to Prevent Spoofing Attacks in VoIP/SIP Networks," *IEEE Access*, vol. 12, pp. 60123–60137, 2024, doi: 10.1109/ACCESS.2024.3393487.

[22] A. Mozo, A. Karamchandani, L. de la Cal, S. Gómez-Canaval, A. Pastor, and L. Gifre, "A Machine-Learning-Based Cyberattack Detector for a Cloud-Based SDN Controller," *Appl. Sci.*, vol. 13, no. 8, 2023, doi: 10.3390/app13084914.

[23] A. Dixit, M. Bhushan, S. Yadav, M. Aggarwal, N. Kalita, and H. Singh, "Impact of Artificial Intelligence and Cyber Security as Advanced Technologies on Bitcoin Industries," *2023 4th Int. Conf. Comput. Autom. Knowl. Manag. ICCAKM 2023*, vol. 12, no. 3, pp. 131–140, 2023, doi: 10.1109/ICCAKM58659.2023.10478539.

[24] M. Lang, L. Connolly, P. Taylor, and P. J. Corner, "The Evolving Menace of Ransomware: A Comparative Analysis of Pre-pandemic and Mid-pandemic Attacks," *Digit. Threat. Res. Pract.*, vol. 4, no. 4, 2023, doi: 10.1145/3558006.

[25] A. Diro, L. Zhou, A. Saini, S. Kaisar, and P. C. Hiep, "Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities," *J. Inf. Secur. Appl.*, vol. 80, 2024, doi: 10.1016/j.jisa.2023.103678.

[26] P. Limna, T. Kraiwanit, K. Jangjarat, P. Klayklung, and P. Chocksathaporn, "The use of ChatGPT in the digital era: Perspectives on chatbot implementation," *J. Appl. Learn. Teach.*, vol. 6, no. 1, pp. 64–74, 2023, doi: 10.37074/jalt.2023.6.1.32.

[27] R. Al-Huthaifi, T. Li, W. Huang, J. Gu, and C. Li, "Federated learning in smart cities: Privacy and security survey," *Inf. Sci. (Ny).*, vol. 632, pp. 833–857, 2023, doi: 10.1016/j.ins.2023.03.033.

[28] Z. Gao, F. Chen, Y. Wang, W. He, X. Shi, and G. Xie, "MVPN: A Defense Architecture against VPN Traffic Hijacking Based on MTD," *Electron.*, vol. 12, no. 3, 2023, doi: 10.3390/electronics12030711.

[29] M. M. Rashid, S. U. Khan, F. Eusufzai, M. A. Redwan, S. R. Sabuj, and M. Elsharief, "A Federated Learning-Based Approach for Improving Intrusion Detection in Industrial Internet of Things Networks," *Network*, vol. 3, no. 1, pp. 158–179, 2023, doi: 10.3390/network3010008.

[30] O. Aouedi, A. Sacco, K. Piamrat, and G. Marchetto, "Handling Privacy-Sensitive Medical Data With Federated Learning: Challenges and Future Directions," *IEEE J. Biomed. Heal. Informatics*, vol. 27, no. 2, pp. 790–803, 2023, doi: 10.1109/JBHI.2022.3185673.

[31] M. Fassl, A. Ponticello, A. Dabrowski, and K. Krombholz, "Investigating Security Folklore: A Case Study on the Tor over VPN Phenomenon," *Proc. ACM Human-Computer Interact.*, vol. 7, no. CSCW2, 2023, doi: 10.1145/3610193.

[32] G. Abbas, U. Farooq, P. Singh, S. S. Khurana, and P. Singh, "Feature Engineering and Ensemble Learning-Based Classification of VPN and Non-VPN-Based Network Traffic over Temporal Features," *SN Comput. Sci.*, vol. 4, no. 5, 2023, doi: 10.1007/s42979-023-01944-5.

[33] N. Bray *et al.*, "A Latency Composition Analysis for Telerobotic Performance Insights Across Various Network Scenarios," *Futur. Internet*, vol. 16, no. 12, 2024, doi: 10.3390/fi16120457.

[34] A. Dhar Dwivedi, R. Singh, K. Kaushik, R. Rao Mukkamala, and W. S. Alnumay, "Blockchain and artificial intelligence for 5G-enabled Internet of Things: Challenges, opportunities, and solutions," *Trans. Emerg. Telecommun. Technol.*, vol. 35, no. 4, 2024, doi: 10.1002/ett.4329.

[35] S. A. A. Mohamed and S. Kurnaz, "Classified VPN Network Traffic Flow Using Time Related to Artificial Neural Network," *Comput. Mater. Contin.*, vol. 80, no. 1, pp. 819–841, 2024, doi: 10.32604/cmc.2024.050474.

[36] Z. A. El Houda, A. S. Hafid, and L. Khoukhi, "MiTFed: A Privacy Preserving Collaborative Network Attack Mitigation Framework Based on Federated Learning Using SDN and Blockchain," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 4, pp. 1985–2001, 2023, doi: 10.1109/TNSE.2023.3237367.

[37] H. Zhang *et al.*, "Classification of Brain Disorders in rs-fMRI via Local-to-Global Graph Neural Networks," *IEEE Trans. Med. Imaging*, vol. 42, no. 2, pp. 444–455, 2023, doi: 10.1109/TMI.2022.3219260.

[38] M. Bahramian, R. K. Dereli, W. Zhao, M. Giberti, and E. Casey, "Data to intelligence: The role of data-driven models in wastewater treatment," 2023. doi: 10.1016/j.eswa.2022.119453.

[39] J. T. Park, C. Y. Shin, U. J. Baek, and M. S. Kim, "Fast and Accurate Multi-Task Learning for Encrypted Network Traffic Classification," *Appl. Sci.*, vol. 14, no. 7, 2024, doi: 10.3390/app14073073.

[40] X. Zheng, X. Ma, Y. Jin, D. Gu, and R. Wang, "Tabular-based self-supervised learning approach for encrypted traffic classification," *J. Electron. Imaging*, vol. 32, no. 04, 2023, doi: 10.1117/1.jei.32.4.043032.

[41] Z. Sui, H. Shu, F. Kang, Y. Huang, and G. Huo, "A Comprehensive Review of Tunnel Detection on Multilayer Protocols: From Traditional to Machine Learning Approaches," *Appl. Sci.*, vol. 13, no. 3, 2023, doi: 10.3390/app13031974.

[42] F. P. E. Putra, U. Ubaidi, A. Hamzah, W. A. Pramadi, and A. Nuraini, "Systematic Literature Review: Security Gap Detection On Websites Using Owasp Zap," *Brill. Res. Artif. Intell.*, vol. 4, no. 1, pp. 348–355, 2024, doi: 10.47709/brilliance.v4i1.4227.

[43] J. Cai, W. Liang, X. Li, K. Li, Z. Gui, and M. K. Khan, "GTxChain: A Secure IoT Smart Blockchain Architecture Based on Graph Neural Network," *IEEE Internet Things J.*, vol. 10, no. 24, pp. 21502–21514, 2023, doi: 10.1109/JIOT.2023.3296469.

[44] B. Mao, J. Liu, Y. Wu, and N. Kato, "Security and Privacy on 6G Network Edge: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 25, no. 2, pp. 1095–1127, 2023, doi: 10.1109/COMST.2023.3244674.

[45] A. K. Bashir *et al.*, "Federated Learning for the Healthcare Metaverse: Concepts, Applications, Challenges, and Future Directions," *IEEE Internet Things J.*, vol. 10, no. 24, pp. 21873–21891, 2023, doi: 10.1109/JIOT.2023.3304790.

[46] K. Wach *et al.*, "The dark side of generative artificial intelligence: A critical analysis of controversies and risks of ChatGPT," *Entrep. Bus. Econ. Rev.*, vol. 11, no. 2, pp. 7–30, 2023, doi: 10.15678/EBER.2023.110201.

[47] O. Aslanli, "Cloud and On-premises Based Security Solution for Industrial IoT," *Int. J. Inf. Eng. Electron. Bus.*, vol. 16, no. 5, pp. 55–62, 2024, doi: 10.5815/IJIEEB.2024.05.02.

[48] A. B. Johal and A. A. Abdulsahib, "Anatomy of Network Security Execution through Utilizing SPSS to Evaluate Public Wi-Fi," *Asia-Pacific J. Inf. Technol. Multimed.*, vol. 12, no. 01, pp. 111–124, 2023, doi: 10.17576/apjitm-2023-1201-06.

[49] P. F. Prasetyo, E. Putra, M. A. Mahmud, and R. Paradina, "Comparing the Performance of LoRaWAN and MQTT Protocols for IoT Sensor Networks," vol. 6, pp. 221–228, 2024, doi: 10.60083/jidt.v6i2.565.
[50] F. Prasetyo, E. Putra, M. Riski, M. S. Yahya, and M. H. Ramadhan, "Mengenal Teknologi Jaringan Nirkabel Terbaru Teknologi 5G," *J. Sistim Inf. dan Teknol.*, vol. 5, no. 2, pp. 167–174, 2023, doi: 10.37034/jsisfotek.v5i1.233.