Vol 3 No. 1 Januari 2026 P-ISSN : 3047-9029 E-ISSN : 3047-9010, Hal 09 – 13

JURNAL RISET SISTEM INFORMASI
Halaman Jurnal: https://journal.smartpublisher.id/index.php/jissi
Halaman UTAMA Jurnal : https://journal.smartpublisher.id

DOI: https://doi.org/10.69714/wf1ema03

IMPLEMENTASI PROTONVPN UNTUK PENINGKATAN KEAMANAN AKSES ONEDRIVE PADA SISTEM OPERASI WINDOWS

Rakhmadi Rahman [a*], Murtafia [b]
[a] Program Studi Sistem Informasi; rakhmadi.rahman@ith.ac.id, Institut Teknologi Bacharuddin Jusuf Habibie; Parepare Sulawesi Selatan
[b] Program Studi Sistem Informasi; Murtafia.221031014@mahasiswa.ac.id, Institut Teknologi Bacharuddin Jusuf Habibie; Parepare Sulawesi Selatan
[*]Penulis Korespondensi: Murtafia

ABSTRACT

As reliance on cloud computing for data management grows, the issue of user data security when accessing services via public networks is a critical concern. This study investigates the implementation of the free-tier version of ProtonVPN on the Windows operating system as a mechanism to reinforce secure access to cloud platforms. ProtonVPN was selected for its offered high-level cryptographic protocols, user-friendly nature, and zero-cost availability. The methodology involved installation, connection configuration, and access testing on major cloud platforms (Google Drive and OneDrive). Results show that using the VPN effectively obfuscates the user's IP address and secures data traffic through encryption, significantly enhancing protection when interacting with cloud services. Despite limitations such as reduced speed performance and limited server choices, this solution proves efficient in elevating the security posture of cloud computing access on Windows devices.

Keywords: *Cloud Computing; Data Security; ProtonVPN; Traffic Encryption.*

Abstrak

Seiring dengan meningkatnya ketergantungan pada komputasi awan untuk penyimpanan dan pemrosesan data, masalah keamanan data pengguna saat mengaksesnya melalui jaringan publik menjadi isu krusial. Penelitian ini mengkaji implementasi ProtonVPN edisi bebas biaya pada sistem operasi Windows sebagai solusi untuk memperkuat pengamanan akses ke layanan awan. Pemilihan ProtonVPN didasarkan pada protokol kriptografi tingkat tinggi yang ditawarkannya, kemudahan penggunaan, dan ketersediaan tanpa biaya. Metodologi penelitian mencakup instalasi, konfigurasi, dan pengujian akses ke platform awan utama (Google Drive dan OneDrive). Hasilnya menunjukkan bahwa penggunaan VPN ini efektif dalam mengaburkan alamat IP pengguna dan mengamankan lalu lintas data melalui penyandian, secara signifikan meningkatkan proteksi saat berinteraksi dengan layanan awan. Meskipun ditemukan adanya penurunan kecepatan dan keterbatasan server, solusi ini terbukti efisien dalam meningkatkan postur keamanan akses komputasi awan pada perangkat Windows.

Kata Kunci: Komputasi Awan; Keamanan Data; ProtonVPN; Penyandian Lalu Lintas.

1. PENDAHULUAN

Komputasi Perkembangan teknologi informasi telah mendorong adopsi komputasi awan (cloud computing) sebagai solusi utama dalam penyimpanan dan pengolahan data. Layanan berbasis awan menawarkan fleksibilitas, skalabilitas, serta efisiensi biaya yang sangat bermanfaat bagi individu maupun organisasi. Namun demikian, meningkatnya ketergantungan pada layanan awan juga membawa tantangan baru, terutama dalam hal keamanan data yang ditransmisikan melalui jaringan publik. Ancaman seperti penyadapan (*eavesdropping*), pencurian data, dan serangan *man-in-the-middle* (MITM) menempatkan data pengguna pada risiko yang signifikan.

Naskah Masuk 3 Oktober 2025; Revisi 4 Oktober 2025; Diterima 7 Oktober 2025; Tersedia 10 Oktober 2025

Untuk mengatasi masalah tersebut, diperlukan mekanisme tambahan yang mampu meningkatkan proteksi lalu lintas data. Salah satu solusi yang umum digunakan adalah Virtual Private Network (VPN)[1]. VPN bekerja dengan cara membangun jalur komunikasi terenkripsi antara perangkat pengguna dan server tujuan, sehingga data yang dikirimkan lebih sulit diakses oleh pihak ketiga. Dari berbagai pilihan VPN yang tersedia, ProtonVPN menjadi salah satu layanan yang menonjol. ProtonVPN menawarkan enkripsi tingkat tinggi, kebijakan tanpa iklan, serta ketersediaan layanan gratis yang dapat diakses pada sistem operasi Windows, termasuk perangkat dengan spesifikasi rendah.

Melalui penelitian ini, dilakukan implementasi ProtonVPN versi gratis pada sistem operasi Windows untuk mengevaluasi sejauh mana solusi ini dapat memperkuat keamanan akses layanan komputasi awan. Penelitian ini menekankan pada tahapan instalasi, konfigurasi, serta pengujian koneksi terhadap layanan awan populer seperti Google Drive dan OneDrive. Dengan demikian, diharapkan hasil penelitian ini dapat memberikan pemahaman mengenai efektivitas penggunaan ProtonVPN sebagai lapisan keamanan tambahan dalam pemanfaatan layanan komputasi awan.

2. TINJAUAN PUSTAKA

Cloud computing telah menghadirkan kemudahan bagi pengguna dalam menyimpan, memproses, serta mengakses data secara fleksibel tanpa harus membangun infrastruktur fisik sendiri. Meski demikian, isu keamanan masih menjadi perhatian utama, terutama dalam menjaga kerahasiaan, integritas, dan ketersediaan data. Berbagai ancaman seperti kebocoran informasi, penyadapan, hingga serangan *man-in-the-middle* (MITM) kerap dilaporkan ketika layanan cloud digunakan melalui jaringan publik [2], [3]. Kondisi ini menuntut adanya lapisan perlindungan tambahan agar data tetap aman saat ditransmisikan.

Salah satu solusi yang banyak digunakan adalah pemanfaatan Virtual Private Network (VPN). Teknologi ini bekerja dengan cara mengenkripsi lalu lintas data dan menyembunyikan alamat IP asli pengguna sehingga aktivitas daring lebih terlindungi. Sejumlah penelitian juga menunjukkan bahwa VPN efektif dalam mencegah intersepsi data pada jaringan Wi-Fi publik serta mampu mengurangi risiko kebocoran identitas digital [4], [5]. Dengan kata lain, VPN berperan penting sebagai gerbang keamanan tambahan bagi pengguna internet, termasuk saat mengakses layanan berbasis cloud.

Dari berbagai penyedia layanan VPN, ProtonVPN menjadi salah satu pilihan populer yang menekankan privasi dan keamanan. Dikembangkan oleh Proton Technologies AG, perusahaan yang juga dikenal dengan layanan ProtonMail, ProtonVPN menawarkan dukungan enkripsi AES-256, protokol OpenVPN dan IKEv2/IPSec, serta kebijakan tanpa pencatatan aktivitas (*no-log*). Fitur ini membuatnya mampu menjaga kerahasiaan data pengguna secara lebih baik. Beberapa penelitian terkini menegaskan bahwa penggunaan ProtonVPN pada perangkat Windows efektif dalam melindungi data saat mengakses layanan *cloud*, meskipun pengguna versi gratis kerap menghadapi keterbatasan dalam hal kecepatan koneksi dan jumlah server yang tersedia [4][6].

3. HASIL DAN PEMBAHASAN

Implementasi ProtonVPN pada sistem operasi Windows memberikan gambaran yang jelas mengenai peningkatan keamanan ketika layanan cloud computing OneDrive diakses melalui jaringan publik. Uji coba dilakukan dengan dua skenario utama: pertama, akses langsung tanpa VPN; kedua, akses dengan VPN aktif.

3.1 Alur Koneksi

Pada skenario pertama (tanpa VPN), lalu lintas data dari Windows menuju server OneDrive berjalan menggunakan alamat IP asli pengguna. Kondisi ini berpotensi menimbulkan risiko, sebab IP dapat dengan mudah dilacak oleh pihak ketiga, sehingga rawan dimanfaatkan dalam serangan berbasis jaringan.
Sebaliknya, setelah VPN diaktifkan, jalur komunikasi dialihkan melalui server ProtonVPN. Alamat IP asli disamarkan dan diganti dengan IP baru dari server VPN. Selain itu, seluruh komunikasi dienkripsi menggunakan protokol aman dengan standar AES-256, sehingga setiap paket yang melintas menjadi jauh lebih sulit untuk dianalisis.

Gambar 1. Alur koneksi Windows – ProtonVPN – OneDrive

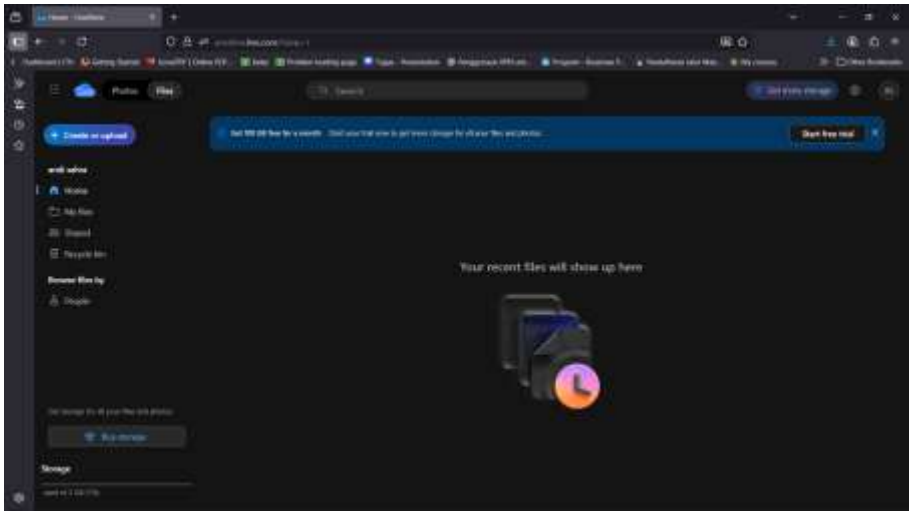
3.2 Aktivasi Proton VPN di Windows

Pengujian menunjukkan bahwa aplikasi ProtonVPN pada Windows dapat diaktifkan tanpa hambatan berarti. Ketika status koneksi berubah menjadi *Connected*, alamat IP publik pengguna langsung berubah. Hal ini menjadi bukti bahwa jalur komunikasi sudah tidak lagi menggunakan IP asli, melainkan melalui server VPN yang berfungsi sebagai *perantara* aman.

Gambar 2.Tampilan Aplikasi ProtonVPN aktif di Windows

3.3 Akses OneDrive Tanpa VPN

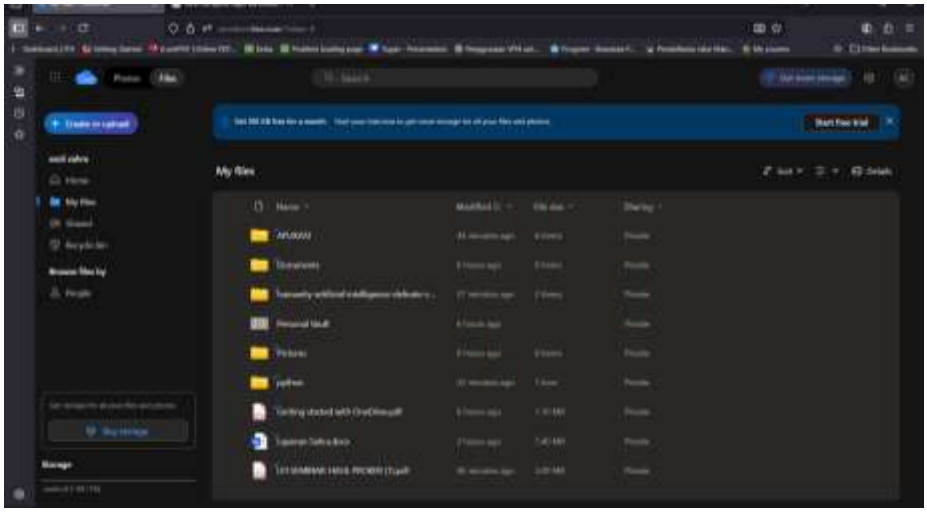
Pada saat OneDrive diakses tanpa VPN, koneksi berlangsung secara normal. Namun, alamat IP publik yang digunakan masih menampilkan identitas asli pengguna. Dari sisi keamanan, kondisi ini tidak optimal, terutama jika akses dilakukan di jaringan terbuka seperti Wi-Fi publik.



Gambar 3. Tampilan OneDrive tanpa VPN

3.4 Akses OneDrive Dengan VPN

Setelah VPN diaktifkan, OneDrive tetap dapat diakses tanpa kendala baik untuk unggah (*upload*) maupun unduh (*download*) file. Perbedaannya terletak pada identitas jaringan: IP publik kini berasal dari server ProtonVPN. Dengan demikian, aktivitas pengguna tersamarkan dan lebih aman dari potensi pelacakan.



Gambar 4. Tampilan OneDrive dengan Proton VPN aktif (IP sudah berubah)

3.5 Analisis Lalu Lintas Data dengan Wireshark

Hasil tangkapan paket menggunakan **Wireshark** memperlihatkan perbedaan mencolok. Tanpa VPN, sebagian besar metadata seperti alamat IP dan jenis protokol masih dapat terlihat dengan jelas. Namun, setelah VPN aktif, paket-paket tersebut berubah menjadi terenkripsi sehingga isi komunikasi tidak dapat diuraikan dengan mudah. Hal ini membuktikan bahwa VPN menambahkan lapisan keamanan ekstra di luar perlindungan bawaan OneDrive.

Gambar 5.Tampilan Wireshark sebelum Proton VPN Diatifkan

Gambar 6. Tampilan Wireshark sesudah Proton VPN diaktifkan

Dari hasil uji, dapat disimpulkan bahwa penggunaan ProtonVPN pada Windows memberikan manfaat nyata dalam meningkatkan keamanan akses OneDrive. Keamanan tidak hanya ditopang oleh enkripsi internal milik layanan cloud Microsoft, tetapi juga diperkuat oleh lapisan proteksi tambahan dari VPN. Dengan adanya penyamaran IP dan enkripsi lalu lintas, risiko serangan *man-in-the-middle* maupun intersepsi data dapat diminimalkan.

Selain itu, fungsi layanan OneDrive tetap berjalan normal sehingga penggunaan VPN tidak menurunkan pengalaman pengguna, melainkan memberikan jaminan kerahasiaan dan integritas data.
halaman.

4. KESIMPULAN DAN SARAN

Hasil penelitian memperlihatkan bahwa penggunaan ProtonVPN pada sistem operasi Windows mampu meningkatkan tingkat keamanan saat mengakses layanan OneDrive sebagai bagian dari *cloud computing*. Dengan mengaktifkan VPN, alamat IP asli pengguna tidak lagi terlihat karena telah digantikan oleh IP milik server ProtonVPN, sementara lalu lintas data diamankan melalui enkripsi tingkat tinggi. Analisis menggunakan Wireshark juga menunjukkan perbedaan yang jelas: tanpa VPN, masih ada informasi yang bisa dikenali dari paket data, tetapi ketika VPN aktif, lalu lintas tersebut berubah menjadi terenkripsi sehingga sulit untuk dipahami oleh pihak ketiga. Kondisi ini menegaskan bahwa ProtonVPN dapat menjadi lapisan perlindungan tambahan di luar mekanisme keamanan bawaan dari OneDrive.

Berdasarkan temuan tersebut, disarankan agar pengguna OneDrive, baik individu maupun kelompok kecil yang sering memanfaatkan jaringan publik, mempertimbangkan penggunaan VPN sebagai langkah pencegahan dari ancaman penyadapan atau serangan berbasis jaringan. ProtonVPN, khususnya versi gratisnya, sudah cukup memberikan perlindungan dasar yang layak digunakan. Untuk pengembangan penelitian berikutnya, akan lebih bermanfaat jika dilakukan perbandingan dengan beberapa layanan VPN lainnya, tidak hanya dari sisi keamanan, tetapi juga stabilitas dan efisiensi kinerjanya. Selain itu, penerapan metode serupa pada layanan *cloud* lain, seperti Google Drive atau Dropbox, dapat memberikan gambaran yang lebih luas mengenai efektivitas VPN dalam menjaga keamanan data di lingkungan komputasi awan.

DAFTAR PUSTAKA

[1] R. M. Pratama, S. Wahyuni, and A. Lubis, “Rancang Bangun Keamanan Koneksi Pribadi Melalui Open VPN Berbasis Cloud,” *INTECOMS J. Inf. Technol. Comput. Sci.*, vol. 6, no. 1, pp. 30–35, 2023, doi: 10.31539/intecoms.v6i1.5368.

[2] R. Gupta, D. Saxena, and A. K. Singh, “Data Security and Privacy in Cloud Computing: Concepts and Emerging Trends,” 2021, [Online]. Available: http://arxiv.org/abs/2108.09508

[3] M. Armbrust *et al.*, “A view of cloud computing,” *Commun. ACM*, vol. 53, no. 4, pp. 50–58, 2010, doi: 10.1145/1721654.1721672.

[4] S. M. Zohaib, S. M. Sajjad, Z. Iqbal, M. Yousaf, M. Haseeb, and Z. Muhammad, “Zero Trust VPN (ZT-VPN): A Systematic Literature Review and Cybersecurity Framework for Hybrid and Remote Work,” *Inf.*, vol. 15, no. 11, 2024, doi: 10.3390/info15110734.

[5] J. Anyam, R. R. Singh, H. Larijani, and A. Philip, “Empirical Performance Analysis of WireGuard vs. OpenVPN in Cloud and Virtualised Environments Under Simulated Network Conditions,” *Computers*, vol. 14, no. 8, 2025, doi: 10.3390/computers14080326.

[6] S. Sutejo, “Implementasi Algoritma Kriptografi Rsa (Rivest Shamir Adleman) Untuk Keamanan Data Rekam Medis Pasien,” *INTECOMS J. Inf. Technol. Comput. Sci.*, vol. 4, no. 1, pp. 104–114, 2021, doi: 10.31539/intecoms.v4i1.2437.