JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER

p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 2357-2366
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.728

Penerapan Virtual Privat Network (VPN) untuk Keamanan Data

Fasrian Mauren Niella Hura[1,*], Agus Damai Lase[2], Devi Chrisman Lase[3]

[1,2,3]Fakultas Sains Dan Teknologi, Eknologi Informasi, Universitas NIAS, Gunungsitoli, Sumatera Utara, Indonesia
Email: [1*]fasrianmaurenniellahura@gmail.com, [2]agusdamailase123@gmail.com, [3]devichrisman@gmail.com
(*EmailCorresponding Author: fasrianmaurenniellahura@gmail.com)
Received: December 14, 2025 | Revision: February 14, 2026 | Accepted: February 14, 2026

Abstrak

Penelitian ini membahas permasalahan keamanan data dan privasi digital yang semakin krusial di tengah meningkatnya aktivitas masyarakat di dunia maya. Melalui metode *library research*, penelitian ini menelaah berbagai literatur ilmiah, jurnal, laporan lembaga keamanan siber, serta sumber akademik lainnya untuk memahami dua isu utama: kerentanan pengguna ketika terhubung pada jaringan publik dan rendahnya tingkat literasi masyarakat terkait mekanisme perlindungan data. Hasil kajian menunjukkan bahwa jaringan publik tetap menjadi salah satu titik paling rentan dalam komunikasi digital karena lemahnya enkripsi dan tingginya risiko intersepsi data. Selain itu, rendahnya pemahaman masyarakat terhadap teknologi perlindungan privasi memperburuk situasi karena pengguna sering kali mengabaikan langkah keamanan demi kenyamanan. Analisis literatur memperlihatkan bahwa perlindungan data tidak hanya bergantung pada teknologi, tetapi juga sangat ditentukan oleh tingkat kesadaran dan pemahaman pengguna. Oleh karena itu, penelitian ini menyimpulkan bahwa solusi keamanan digital harus mengintegrasikan aspek teknologi dan edukasi secara seimbang. Dengan pendekatan tersebut, pengguna dapat lebih memahami risiko yang dihadapi sekaligus mampu memanfaatkan teknologi perlindungan dengan lebih efektif untuk menjaga privasi digital mereka.

Kata kunci: Keamanan Data, Enkripsi Data, Perlindungan Data Pribadi, Privasi Digital, Virtual Privat Network(VPN)

Abstract

This study addresses the increasingly crucial issues of data security and digital privacy amidst the rise in online activity. Using library research, the study examined various scientific literature, journals, cybersecurity agency reports, and other academic sources to understand two key issues: user vulnerability when connecting to public networks and the low level of public literacy regarding data protection mechanisms. The study's findings indicate that public networks remain one of the most vulnerable points in digital communication due to weak encryption and the high risk of data interception. Furthermore, the public's lack of understanding of privacy protection technology exacerbates the situation, as users often neglect security measures for the sake of convenience. The literature analysis demonstrates that data protection is not solely dependent on technology but is also largely determined by users' awareness and understanding. Therefore, this study concludes that digital security solutions must balance technological and educational aspects. This approach will help users better understand the risks they face and utilize protection technology more effectively to safeguard their digital privacy.

Keywords: *Data Security, Data Encryption, Personal Data Protection, Digital Privacy, Virtual Private Network (VPN)*

1. PENDAHULUAN

Di tengah perkembangan modernisasi yang semakin tergantung pada teknologi digital, masalah keamanan data dan perlindungan privasi informasi menjadi isu penting dalam kegiatan masyarakat di dunia maya[1], [2], [3]. Semua kegiatan digital, seperti bekerja, belajar, berkomunikasi, dan melakukan transaksi, sangat bergantung pada koneksi internet. Kondisi ini memerlukan adanya mekanisme perlindungan data yang mampu memastikan kerahasiaan, integritas, dan keamanan informasi pengguna. Salah satu teknologi yang sering digunakan untuk tujuan tersebut adalah Virtual Private Network (VPN).

VPN adalah teknologi jaringan yang digunakan untuk membentuk saluran komunikasi yang aman melalui jaringan umum. Teknologi ini bekerja dengan cara mengenkripsi data yang dikirim dan menyembunyikan identitas pengguna yang menggunakan layanan tersebut[4]. Teknologi ini memungkinkan pengguna mengakses internet atau jaringan internal dengan lebih aman, khususnya ketika terhubung ke jaringan publik yang kurang memiliki keamanan yang memadai[5], [6]. VPN dipilih sebagai topik penelitian karena memiliki sifat yang fleksibel, relatif mudah digunakan, dapat diaplikasikan pada berbagai jenis perangkat, serta cocok digunakan oleh pengguna pemula maupun organisasi yang membutuhkan perlindungan data tanpa memerlukan konfigurasi teknis yang rumit. Peningkatan penggunaan jaringan internet seiring dengan meningkatnya berbagai ancaman siber, seperti kebocoran data pribadi, peretasan akun, penyadapan komunikasi, dan manipulasi informasi. Berbagai laporan mengenai pelanggaran keamanan menunjukkan bahwa ancaman tersebut benar-benar nyata dan mungkin terjadi dalam aktivitas digital sehari-hari. Penggunaan jaringan Wi-Fi publik di tempat seperti kafe, bandara, hotel, atau fasilitas umum sering kali menjadi celah keamanan karena tingkat

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 2357-2366
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.728

enkripsi yang rendah dan kontrol akses yang tidak cukup memadai. Dalam situasi ini, data pengguna berisiko disadap atau digunakan oleh pihak yang tidak dapat dipercaya.

Selain masalah teknis, keamanan data juga terganggu karena masyarakat kurang memahami cara perlindungan privasi digital[7], [8]. Banyak orang yang menggunakan internet belum menyadari bahwa tindakan-tindakan sehari-hari seperti mengakses situs web, masuk ke aplikasi, atau melakukan pembelian secara daring bisa berpotensi menyebabkan kebocoran data jika tidak dilindungi dengan langkah tambahan. Kurangnya pemahaman tentang literasi digital menyebabkan banyak pengguna mengabaikan langkah-langkah keamanan hanya demi rasa nyaman, sehingga membuat mereka lebih rentan terhadap berbagai ancaman siber[9].

Dalam konteks tersebut, penggunaan VPN menjadi solusi yang tepat karena mampu melindungi data dengan cara mengenkripsi informasi dan membuat jalur terenkripsi tanpa secara signifikan mengurangi kenyamanan pengguna. Berbeda dengan solusi keamanan lain yang biasanya membutuhkan infrastruktur khusus atau pemahaman teknis yang tinggi,VPN bisa diaplikasikan secara luas dan praktis. Oleh karena itu, penelitian mengenai penerapan Virtual Private Network (VPN) sebagai cara melindungi data perlu dilakukan secara mendalam, terutama mengingat semakin tingginya ancaman keamanan di jaringan publik[10].

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis peranVPN dalam meningkatkan keamanan data serta privasi digital dengan menggunakan pendekatan penelitian berupa studi pustaka. Penelitian ini mengkaji berbagai sumber ilmiah untuk memahami sejauh mana tingkat kerentanan pengguna terhadap jaringan publik serta rendahnya kesadaran masyarakat tentang perlindungan data. Dengan demikian, diharapkan penelitian ini dapat memberikan gambaran yang lebih jelas mengenai pentingnya penggunaan VPN sebagai solusi keamanan digital yang mudah diterapkan dan sesuai dengan kebutuhan pengguna pada masa kini.Ketidakstabilan keamanan pada infrastruktur jaringan publik menjadi salah satu faktor yang paling memicu kekhawatiran, khususnya ketika pengguna terhubung pada jaringan umum di bandara, kafe, atau fasilitas publik lainnya[11].

Dalam konteks penelitian ini, kebutuhan akan solusi keamanan yang lebih kuat dan adaptif melahirkan relevansi untuk menghadirkan teknologi yang mampu memberikan lapisan perlindungan tambahan[12], [13]. Berbagai pendekatan telah ditawarkan oleh komunitas keamanan digital, mulai dari enkripsi komunikasi, firewall, hingga sistem deteksi ancaman berbasis kecerdasan buatan. Namun, sebagian dari solusi tersebut memerlukan pengetahuan teknis tinggi atau infrastruktur pendukung yang tidak dapat diakses oleh semua kalangan. Oleh karena itu, penelitian mengenai mekanisme perlindungan yang lebih mudah diadopsi masyarakat luas menjadi semakin penting untuk dilakukan.

Sejalan dengan meningkatnya kebutuhan tersebut, banyak penelitian dan inovasi lahir untuk menemukan cara paling efektif dalam menjaga kerahasiaan data saat terhubung ke jaringan internet. Berbagai metode keamanan telah dibandingkan dan dievaluasi, namun semuanya pada dasarnya memiliki tujuan yang sama: memberikan proteksi yang dapat diandalkan saat pengguna melakukan komunikasi digital. Penelitian sebelumnya menunjukkan bahwa pendekatan yang mengandalkan *tunneling*, enkripsi, dan penyembunyian identitas jaringan menjadi salah satu metode yang cukup konsisten dalam meningkatkan keamanan pengguna tanpa mengganggu kenyamanan mereka[14], [15].

Selain itu, perkembangan teknologi global menunjukkan meningkatnya tren penggunaan alat keamanan yang bersifat fleksibel, dapat dipasang di berbagai perangkat, dan mampu bekerja pada beragam kondisi jaringan. Banyak studi yang berfokus pada bagaimana mengamankan lalu lintas data dari upaya penyadapan, mencegah pencurian identitas, serta melindungi akses pengguna saat mengunjungi situs maupun layanan daring.[1] Hal ini mencerminkan bahwa dunia riset telah lama mengakui pentingnya keberadaan mekanisme yang membantu menjaga privasi digital secara praktis.

Tak dapat dipungkiri, berbagai penelitian terkait keamanan siber menunjukkan bahwa perlindungan data tidak hanya berfungsi sebagai pelindung dari ancaman, tetapi juga sebagai pondasi terciptanya lingkungan digital yang lebih sehat. Ketika pengguna merasa aman, mereka dapat memanfaatkan internet secara lebih optimal untuk bekerja, belajar, maupun berkolaborasi tanpa rasa khawatir akan risiko penyalahgunaan informasi. Teknologi keamanan yang baik harus mampu memberikan rasa kepercayaan tersebut.

Penelitian ini juga berangkat dari berbagai pekerjaan terdahulu yang mengkaji bagaimana teknologi pelindung identitas dan pengaman jalur komunikasi menjadi salah satu standar dalam dunia jaringan modern. Beberapa solusi yang telah ada terbukti efektif, namun sebagian lainnya memiliki keterbatasan terkait kemudahan penggunaan, kecepatan akses, biaya, ataupun kompatibilitas. Dengan memahami peluang dan kekurangan berbagai pendekatan sebelumnya, penelitian ini berupaya menghadirkan pandangan yang lebih jelas mengenai pentingnya solusi yang lebih adaptif, lebih inklusif, dan lebih ramah bagi pengguna umum.

Melalui latar belakang tersebut, pendahuluan ini menggarisbawahi bahwa upaya menjaga keamanan data merupakan sebuah kebutuhan fundamental yang tidak dapat ditunda. Masyarakat memerlukan sistem yang mampu melindungi privasi dan menjaga integritas data dalam situasi apa pun. Kehadiran solusi yang tepat diharapkan dapat memberikan jawaban atas berbagai keresahan yang berkembang dalam ruang digital, serta memperkuat kepercayaan masyarakat dalam memanfaatkan teknologi.

Di tengah dinamika perkembangan dunia digital yang semakin cepat, terdapat sejumlah persoalan utama yang menjadi pemicu pentingnya penelitian mengenai keamanan data. Permasalahan pertama muncul dari meningkatnya kerentanan pengguna ketika terhubung ke jaringan publik yang tidak memiliki kontrol keamanan memadai. Banyak kasus

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 2357-2366
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.728

menunjukkan bahwa jaringan tersebut sering menjadi pintu masuk bagi pihak tidak bertanggung jawab untuk menyusup ke perangkat pengguna dan mengambil informasi sensitif tanpa disadari.[2] Kondisi ini semakin memperlihatkan betapa rentannya data ketika berpindah melalui jalur komunikasi yang tidak terproteksi dengan baik.

Permasalahan kedua yang melatarbelakangi penelitian ini adalah minimnya pemahaman masyarakat mengenai alat atau mekanisme yang dapat digunakan untuk menjaga privasi digital mereka. Walaupun banyak teknologi perlindungan telah tersedia, tidak semua pengguna mengetahui cara kerja, manfaat, ataupun alasan mengapa teknologi tersebut penting digunakan. Kurangnya literasi ini berdampak pada rendahnya tingkat adopsi perlindungan data di tingkat individu, padahal aktivitas digital terus meningkat setiap hari. Situasi ini menimbulkan kebutuhan untuk menghadirkan penjelasan yang lebih komprehensif mengenai teknologi yang mampu memberikan perlindungan tambahan dalam koneksi jaringan.

Berdasarkan permasalahan tersebut, penelitian ini memiliki beberapa tujuan yang ingin dicapai. Tujuan pertama adalah memberikan pemahaman yang lebih jelas dan terstruktur mengenai peran teknologi perlindungan jaringan dalam menjaga keamanan dan privasi data pengguna. Penelitian berupaya menjelaskan konsep dasar, prinsip kerja, serta alasan mengapa teknologi tersebut menjadi bagian penting dalam sistem keamanan modern, tanpa membahas aspek teknis secara mendalam pada tahap pendahuluan.

Tujuan kedua dari penelitian ini adalah mengkaji berbagai literatur yang berkaitan dengan mekanisme pengamanan data untuk menghasilkan gambaran menyeluruh mengenai efektivitas, relevansi, serta perkembangan penggunaan teknologi tersebut dalam konteks keamanan digital. Dengan menggabungkan temuan dari penelitian terdahulu, penelitian ini diharapkan dapat memberikan landasan yang kuat untuk memahami bagaimana perlindungan data dapat diterapkan secara lebih efisien dan sesuai kebutuhan masyarakat masa kini.

Melalui perumusan permasalahan dan tujuan tersebut, pendahuluan ini semakin menegaskan bahwa penelitian mengenai keamanan data bukan hanya sekadar telaah teoretis, tetapi juga respons terhadap kebutuhan nyata pengguna internet. Penelitian ini diharapkan dapat memberikan kontribusi pada upaya meningkatkan kesadaran, pemahaman, dan kesiapan masyarakat dalam menghadapi tantangan keamanan digital yang terus berkembang.

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan *library research* atau penelitian kepustakaan, yaitu metode yang berfokus pada pengumpulan, analisis, dan sintesis berbagai sumber tertulis yang relevan. Pendekatan ini memungkinkan peneliti memperoleh pemahaman yang mendalam mengenai konsep, teori, dan temuan penelitian sebelumnya terkait keamanan data serta teknologi yang digunakan dalam menjaga privasi komunikasi digital. Melalui eksplorasi literatur, peneliti dapat menelaah perkembangan keilmuan, mengidentifikasi celah penelitian, serta menyusun pemahaman yang komprehensif mengenai isu yang dikaji.

Library research dipilih karena topik yang diteliti memiliki landasan teoritis dan teknis yang luas, sehingga memerlukan eksplorasi literatur yang bersumber dari jurnal akademik, buku referensi, laporan penelitian, standar keamanan internasional, artikel ilmiah, hingga dokumentasi teknis dari lembaga dan organisasi terkait keamanan siber. Penelitian ini tidak melakukan eksperimen lapangan, melainkan fokus pada analisis konsep dan temuan yang sudah ada.

Kerangka penelitian ini dibuat dengan tujuan untuk menjelaskan proses berpikir dalam penelitian mengenai penerapan Virtual Private Network (VPN) sebagai sarana meningkatkan keamanan data serta privasi digital pengguna internet, terutama pada jaringan yang bersifat publik.

a. Kondisi Awal (Permasalahan Utama)

Peningkatan penggunaan jaringan internet dalam berbagai kegiatan digital berdampak pada peningkatan potensi ancaman siber, seperti:

1. Kebocoran data pribadi
2. Peretasan akun
3. Penyadapan komunikasi
4. Manipulasi informasi

Ancaman tersebut semakin meningkat ketika pengguna terhubung ke jaringan Wi-Fi publik yang biasanya memiliki:

1. Tingkat enkripsi rendah
2. Kontrol akses yang lemah
3. Pengawasan keamanan yang terbatas

Akibatnya, data pengguna dapat dengan mudah disadap atau digunakan secara tidak sah oleh pihak-pihak yang tidak bertanggung jawab.

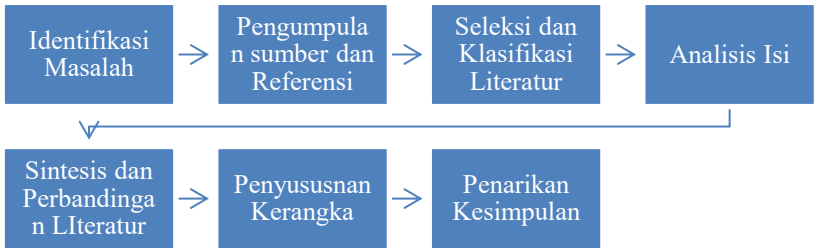
b. Faktor Pendukung Permasalahan

Selain aspek teknis jaringan, kerentanan keqamanan data juga dipengaruhi oleh faktor-faktor lainnya.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 2357-2366
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.728

1. Rendahnya literasi digital masyarakat
2. Minimnya pemahaman tentang perlindungan privasi digital
3. Kecenderungan pengguna mengutamakan kenyamanan dibandingkan keamanan
4. Kondisi ini membuat pengguna cenderung mengesampingkan langkah-langkah perlindungan data, akibatnya risiko ancaman siber semakin besar.

2.1 Tahapan Penelitian



Gambar 1. Tahapan Penelitian

a. Identifikasi Masalah
Tahap awal dilakukan dengan mengidentifikasi permasalahan utama yang berkaitan dengan keamanan data pada jaringan internet. Peneliti meninjau fenomena terkini, kasus-kasus pelanggaran keamanan, dan alasan mengapa perlindungan data menjadi krusial di era digital.

b. Pengumpulan Sumber dan Referensi
Peneliti mengumpulkan berbagai sumber literatur yang relevan dari perpustakaan fisik maupun digital. Sumber yang digunakan meliputi jurnal ilmiah, prosiding konferensi, buku teks, laporan lembaga keamanan siber, dan publikasi akademik internasional yang membahas keamanan jaringan dan mekanisme perlindungan data.

c. Seleksi dan Klasifikasi Literatur
Literatur yang terkumpul kemudian diseleksi berdasarkan relevansi, kredibilitas, dan mutakhirnya informasi. Setelah itu dilakukan pengelompokan sumber berdasarkan tema tertentu, seperti konsep dasar keamanan jaringan, tren ancaman digital, teknologi yang digunakan untuk perlindungan data, serta penelitian terkait yang pernah dilakukan sebelumnya.

d. Analisis Isi (*Content Analysis*)
Pada tahap ini, peneliti melakukan pembacaan mendalam terhadap seluruh literatur terpilih. Analisis dilakukan untuk memahami teori, metode, temuan penelitian, dan kesimpulan yang pernah dikemukakan oleh para peneliti sebelumnya. Pendekatan *content analysis* digunakan untuk mengekstraksi gagasan utama dari setiap sumber.

e. Sintesis dan Perbandingan Literatur
Peneliti menyusun temuan-temuan dari berbagai sumber secara sistematis, lalu membandingkan perbedaan, persamaan, serta kekuatan dan keterbatasan masing-masing penelitian. Sintesis ini membantu membangun pemahaman yang terstruktur mengenai isu yang dikaji serta memetakan perkembangan dan arah penelitian sebelumnya.

f. Penyusunan Kerangka Pemikiran
Berdasarkan hasil sintesis, peneliti membentuk kerangka pemikiran yang menjadi dasar bagi penjelasan dan penarikan kesimpulan. Kerangka ini membantu menghubungkan temuan penelitian terdahulu dengan fokus penelitian yang sedang dilakukan.

g. Penarikan Kesimpulan
Tahap akhir adalah menyusun kesimpulan berdasarkan hasil analisis literatur. Kesimpulan mencerminkan rangkuman temuan, kontribusi penelitian, serta rekomendasi untuk penelitian selanjutnya.

2.2 Metode Penyelesaian Masalah

Metode penyelesaian masalah dalam penelitian berbasis *library research* ini dilakukan melalui beberapa pendekatan:

a. Pendekatan Analitis Deskriptif
Masalah diselesaikan dengan cara mendeskripsikan berbagai konsep dan teori terkait keamanan data, kemudian menganalisisnya secara kritis berdasarkan referensi yang ada. Pendekatan ini membantu menjelaskan bagaimana literatur yang tersedia menjawab isu yang sedang dikaji.

b. Pendekatan Komparatif

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 2357-2366
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.728

Peneliti membandingkan berbagai solusi dan temuan dari penelitian sebelumnya. Perbandingan dilakukan untuk menemukan pola, efektivitas pendekatan, serta celah yang masih menjadi perhatian dalam pengembangan teknologi keamanan jaringan.

c. Pendekatan Sintesis Teoritis

Berbagai informasi dari literatur kemudian digabungkan untuk menghasilkan pemahaman baru yang lebih utuh. Sintesis teoritis ini membantu menyusun gambaran komprehensif tentang bagaimana solusi keamanan digital dikembangkan dan diterapkan.

d. Formulasi Pemecahan Masalah

Berdasarkan hasil analisis dan sintesis, peneliti merumuskan solusi konseptual yang dianggap paling sesuai untuk menjawab permasalahan yang dikaji. Solusi ini tidak berupa implementasi teknis, tetapi berupa pemahaman konseptual berdasarkan literatur terverifikasi.

3. HASIL DAN PEMBAHASAN

3.1 Pengertian Virtual Privat Network(VPN)

Virtual Private Network, atau yang lebih dikenal dengan VPN, merupakan sebuah teknologi yang dirancang untuk menciptakan jalur komunikasi yang aman dan privat ketika pengguna terhubung ke jaringan internet. Pada dasarnya, VPN berfungsi sebagai penghubung yang memungkinkan pengguna mengakses jaringan publik seolah-olah mereka sedang berada di dalam jaringan khusus yang tertutup dan terlindungi. Konsep ini hadir sebagai jawaban atas kebutuhan masyarakat modern untuk menjaga privasi dan kerahasiaan data mereka di tengah lingkungan digital yang semakin terbuka dan rentan terhadap ancaman.

Secara umum, VPN dapat dipahami sebagai sebuah layanan yang memberikan ruang aman bagi pengguna untuk menjalankan aktivitas daring tanpa perlu khawatir mengenai potensi penyadapan atau pemantauan dari pihak lain. Teknologi ini bekerja dengan memastikan bahwa hubungan antara perangkat pengguna dan jaringan yang dituju berada dalam kondisi yang terlindungi dari akses yang tidak sah. Dengan demikian, informasi yang dipertukarkan selama proses komunikasi digital terjaga kerahasiaannya meskipun melewati jaringan yang tidak selalu aman, seperti jaringan publik.

Ada beberapa pengertian VPN Menurut para ahli, antara lain :

a. menurut penjelasan (suhendar, 2016), vpn dipahami sebagai teknologi yang memungkinkan pengguna untuk terhubung ke jaringan lokal meskipun mereka berada di luar lokasi fisik jaringan tersebut. melalui koneksi internet, pengguna dapat mengakses sumber daya yang tersedia pada jaringan lokal dan memperoleh hak akses yang sama seperti ketika berada langsung di dalam jaringan tersebut. dengan cara ini, vpn memberikan fleksibilitas bagi individu atau organisasi untuk melakukan aktivitas digital dari jarak jauh tanpa kehilangan kendali terhadap sumber daya jaringan.
b. sofana memberikan gambaran bahwa vpn pada dasarnya adalah teknologi jaringan yang memungkinkan beberapa jaringan lokal yang secara fisik terpisah dan berjauhan untuk saling terhubung melalui media komunikasi publik seperti internet. penjelasan ini menekankan bahwa vpn bekerja dengan memanfaatkan jaringan umum, tetapi menciptakan jalur yang seolah-olah bersifat privat. salah satu aspek penting dari penjelasan sofana adalah konsep *tunneling*. melalui proses ini, data yang dikirimkan dari satu titik ke titik lainnya dibungkus dengan protokol khusus sehingga tidak dapat dibaca oleh pihak yang tidak berkepentingan. “pembungkusan” tersebut memungkinkan data tetap aman meskipun melalui jaringan yang tidak terjamin keamanannya. dengan kata lain, sofana menekankan sisi keamanan dan privasi yang menjadi inti dari keberadaan vpn.
c. menurut putra dan rekan-rekan, vpn adalah teknologi komunikasi yang digunakan untuk menghubungkan pengguna ke sebuah jaringan lokal setelah mereka lebih dulu terhubung ke jaringan publik. definisi ini memberikan sudut pandang yang menekankan proses akses: pengguna tidak langsung masuk ke jaringan lokal, tetapi melalui jaringan publik sebagai perantara. hal ini memberikan gambaran bahwa vpn menjadi semacam jembatan yang memungkinkan pengguna merasa “masuk” ke jaringan yang sebenarnya berada jauh dari lokasi fisik mereka. penjelasan ini menyoroti fleksibilitas vpn dalam menyediakan akses jarak jauh yang aman, sangat berguna bagi pekerja, lembaga pendidikan, maupun organisasi yang memerlukan koneksi internal tanpa harus berada di lokasi fisik jaringan tersebut.
d. dalam pandangan umam dan roza, vpn dikaitkan langsung dengan penggunaan teknologi gre (*generic routing encapsulation*) tunnel. gre adalah protokol yang digunakan untuk mengemas berbagai jenis paket data agar dapat dikirim melalui jaringan antar-router. pendekatan ini menjelaskan sisi teknis vpn yang berfungsi bukan hanya sebagai alat untuk menyembunyikan data, tetapi juga sebagai teknologi yang memungkinkan hubungan antarmesin atau antarruter secara fleksibel. penggunaan gre membuat pengiriman paket menjadi lebih seragam dan stabil karena protokol ini mampu membawa berbagai tipe data dalam satu jalur yang tersusun. Pandangan ini menekankan bahwa di balik konsep VPN terdapat mekanisme jaringan yang kompleks untuk memungkinkan komunikasi antar-node secara aman dan efisien.

Dari pengertian ahli diatas bahwa Virtual Private Network (VPN) dapat disimpulkan sebagai sebuah teknologi jaringan yang berfungsi menciptakan jalur komunikasi yang aman, privat, dan terlindungi ketika pengguna terhubung ke jaringan publik seperti internet. Walaupun memanfaatkan infrastruktur jaringan umum, VPN membangun lingkungan “virtual” yang menyerupai jaringan lokal tertutup, sehingga pengguna tetap dapat mengakses sumber daya

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 2357-2366
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.728

internal secara aman dari jarak jauh. Inti dari teknologi ini terletak pada kemampuannya melakukan *tunneling* atau pembungkusan data, yaitu proses yang memastikan informasi yang dikirim tidak dapat dengan mudah dibaca, dimodifikasi, atau disadap oleh pihak yang tidak berwenang.

Selain memberikan akses jarak jauh, VPN juga menekankan keamanan sebagai aspek utamanya. Setiap transmisi data yang melewati internet harus terlindungi dari akses pihak yang tidak berwenang. Oleh karena itu, teknologi ini selalu dilengkapi dengan fitur inti berupa enkripsi dan tunneling. Enkripsi berfungsi menjaga kerahasiaan data agar tidak dapat dibaca oleh pihak yang tidak berhak, sementara tunneling menciptakan jalur khusus yang aman untuk mengirimkan data. Dengan dua mekanisme ini, VPN memastikan bahwa komunikasi digital tetap terjaga keamanannya meskipun melalui jaringan publik.

VPN tidak hanya berkaitan dengan perlindungan data, tetapi juga erat dengan konsep privasi digital. Ketika seseorang menggunakan jaringan internet, identitas digitalnya dapat dilacak melalui berbagai parameter. Dalam konteks inilah VPN berperan sebagai alat yang membantu menyamarkan jejak digital pengguna sehingga aktivitas daring menjadi lebih sulit untuk diidentifikasi oleh pihak-pihak tertentu. Hal ini menjadikan VPN sebagai pilihan banyak individu maupun organisasi dalam memastikan bahwa aktivitas mereka tetap berada dalam lingkup yang aman dan tidak mudah terawasi.

Konsep VPN juga berkaitan dengan gagasan konektivitas yang lebih fleksibel. Banyak pengguna memanfaatkan VPN untuk mengakses jaringan tertentu dari jarak jauh, seolah-olah mereka sedang berada di lokasi yang sama dengan jaringan tersebut. Hal ini memungkinkan pekerja, pelajar, maupun individu yang memerlukan akses ke lingkungan digital tertentu untuk tetap terhubung secara aman di mana pun mereka berada.[16] Oleh karena itu, VPN tidak hanya dipahami sebagai alat keamanan, tetapi juga sebagai sarana pendukung mobilitas digital.

Dalam dunia bisnis, pengertian VPN semakin meluas karena penggunaannya tidak lagi terbatas pada perlindungan data pribadi. Organisasi memanfaatkan VPN untuk menjaga agar komunikasi internal tetap berada dalam wilayah yang terkontrol. Dengan begitu, informasi penting perusahaan tidak mudah diakses oleh pihak eksternal, sekalipun seluruh kegiatan dilakukan melalui jaringan internet global. Penggunaan ini menunjukkan bahwa VPN telah menjadi bagian penting dalam tata kelola keamanan informasi modern

Secara keseluruhan, VPN dapat dipandang sebagai fondasi yang memungkinkan terciptanya pengalaman berselancar di internet yang lebih aman, lebih privat, dan lebih terarah. Teknologi ini hadir bukan hanya sebagai perangkat tambahan, tetapi sebagai bagian dari kebutuhan dasar pengguna digital yang memprioritaskan keamanan informasi. Dalam dunia yang terus berkembang, definisi VPN semakin meluas, tetapi inti utamanya tetap sama: memberikan perlindungan dan kenyamanan ketika terhubung ke jaringan internet.

3.2 Kerentanan Pengguna pada Jaringan Publik

Permasalahan meningkatnya kerentanan pengguna ketika terhubung ke jaringan publik telah menjadi isu yang sering dibahas dalam berbagai literatur keamanan digital. Penelitian-penelitian terdahulu menggambarkan bahwa jaringan public seperti Wi-Fi gratis di kafe, pusat perbelanjaan, bandara, hotel, dan fasilitas umum merupakan salah satu lingkungan yang paling rentan terhadap serangan siber. Dalam *library research*, persoalan ini dipahami melalui penelaahan sumber-sumber ilmiah yang menunjukkan bagaimana struktur jaringan publik pada umumnya tidak dilengkapi protokol keamanan yang memadai, sehingga memudahkan pihak asing untuk mengakses lalu lintas data pengguna tanpa terdeteksi.

Banyak literatur yang menekankan bahwa jaringan publik sering kali tidak menerapkan enkripsi yang kuat pada data yang dikirimkan antarperangkat. Ketika literatur keamanan membahas tentang "*open networks*" atau jaringan terbuka, sebagian besar mengaitkannya dengan potensi serangan seperti *man-in-the-middle attack*, *packet sniffing*, dan *session hijacking*. Melalui pendekatan analitis-deskriptif dalam penelitian kepustakaan, konsep-konsep tersebut dijelaskan bukan berdasarkan percobaan langsung, melainkan berdasarkan dokumentasi ilmiah yang menggambarkan pola serangan yang sudah teridentifikasi dalam berbagai studi keamanan jaringan.

Dalam tinjauan literatur lainnya, ditemukan bahwa banyak serangan yang memanfaatkan kelemahan struktur jaringan publik dengan cara menempatkan perangkat penyadap pada titik akses yang sama dengan pengguna. Peneliti keamanan siber dalam berbagai jurnal menyebut bahwa serangan tersebut sangat efektif karena pengguna tidak dapat membedakan antara jaringan yang sah dan jaringan palsu (*rogue access point*).[17] Dengan demikian, perangkat pengguna sering kali terhubung secara otomatis tanpa memeriksa legitimasi jaringan, dan hal ini membuka jalan bagi penyerang untuk membaca bahkan memodifikasi lalu lintas data.

Selain itu, analisis literatur juga menunjukkan bahwa aktivitas digital pengguna seperti login ke aplikasi, mengirim pesan, membuka akun bank, atau mengunduh berkas tertentu dapat dengan mudah dipantau apabila koneksi tidak dilindungi oleh metode perlindungan yang memadai. Penelitian terdahulu menggambarkan bahwa data yang tidak dienkripsi dapat dibaca seolah-olah dalam bentuk teks biasa, sehingga sangat rentan untuk dicuri atau dimanipulasi. Dalam konteks inilah para pakar keamanan dalam berbagai publikasi mengingatkan bahwa jaringan publik sebaiknya tidak digunakan untuk aktivitas yang melibatkan informasi sensitif.

Melalui pendekatan komparatif dalam library research, ditemukan bahwa berbagai studi menunjukkan tingkat ancaman yang berbeda-beda tergantung jenis jaringan dan model serangan yang digunakan. Namun, semuanya sepakat

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 2357-2366
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.728

bahwa jaringan publik tetap menjadi titik paling lemah dalam sistem keamanan digital secara keseluruhan. Banyak penelitian bahkan menyoroti bahwa pengguna sering kali tidak sadar bahwa ancaman tersebut benar-benar nyata, karena serangan terhadap jaringan publik cenderung tidak terlihat dan tidak menimbulkan gejala yang langsung disadari oleh korban.

Literatur lain juga menyoroti faktor kebiasaan pengguna sebagai elemen penting dari persoalan ini. Banyak sumber menjelaskan bahwa kenyamanan akses gratis membuat pengguna mengabaikan keamanan, sehingga menciptakan kesenjangan besar antara pemahaman risiko dan perilaku digital sehari-hari. Dalam penelitian kepustakaan, pola perilaku ini tidak diukur melalui survei lapangan, melainkan dikaji berdasarkan temuan-temuan psikologi pengguna teknologi dan laporan kasus yang terdokumentasi oleh lembaga keamanan siber.

Dengan menggabungkan temuan-temuan tersebut melalui proses sintesis teoritis, dapat dipahami bahwa meningkatnya kerentanan pada jaringan publik bukan hanya disebabkan oleh kelemahan teknis, tetapi juga minimnya kesadaran pengguna mengenai mekanisme perlindungan data. Salah satu kesimpulan umum dari berbagai literatur adalah bahwa jalur komunikasi yang tidak terlindungi membuka ruang bagi pihak luar untuk melakukan intersepsi data, baik secara pasif maupun aktif.

Dalam konteks pembahasan ini, permasalahan kerentanan jaringan publik menjadi dasar penting mengapa perlindungan tambahan sangat dibutuhkan. Berbagai literatur menunjukkan bahwa tanpa perlindungan, aktivitas digital pengguna dapat diakses dengan mudah oleh pihak tidak berwenang. Fakta ilmiah dari penelitian-penelitian sebelumnya secara konsisten menegaskan bahwa keamanan data dalam jaringan publik tidak dapat dijamin, dan pengguna yang sering terhubung tanpa perlindungan memiliki risiko jauh lebih tinggi mengalami pencurian data, penyadapan, atau pengambilalihan akun.

Dengan demikian, melalui pendekatan library research, pembahasan ini menegaskan bahwa jaringan publik adalah salah satu titik paling rawan dalam keamanan digital modern, dan literatur-litetatur akademik maupun teknis telah banyak menguraikan bagaimana kerentanannya dapat dimanfaatkan oleh penyerang. Pemahaman tersebut menjadi fondasi bagi pembahasan selanjutnya dalam penelitian.

3.3 Minimnya Pemahaman Masyarakat tentang Mekanisme Perlindungan Privasi Digital

Minimnya pemahaman masyarakat mengenai alat atau mekanisme perlindungan privasi digital merupakan isu yang banyak dibahas dalam literatur keamanan informasi. Melalui penelitian kepustakaan, berbagai sumber ilmiah menunjukkan bahwa meskipun teknologi perlindungan data berkembang dengan sangat pesat, tingkat literasi digital masyarakat tidak selalu mengikuti perkembangan tersebut. Kondisi ini menciptakan kesenjangan yang signifikan antara ketersediaan teknologi keamanan dan kemampuan pengguna untuk memanfaatkannya secara efektif. Sejumlah publikasi menekankan bahwa kurangnya edukasi, minimnya sosialisasi, serta kompleksitas informasi teknologi menjadi faktor utama yang menghambat pemahaman pengguna.

Dalam berbagai referensi akademik, disebutkan bahwa salah satu penyebab rendahnya literasi keamanan digital adalah sifat teknologi yang sering dianggap terlalu teknis dan sulit dijangkau oleh pengguna awam. Banyak pengguna yang bahkan tidak mengetahui bahwa data pribadi mereka terus berpindah-pindah melewati berbagai server dan jaringan, sehingga risiko kebocoran data menjadi hal yang tak terhindarkan apabila tidak ada perlindungan tambahan. Literasi mengenai risiko ini umumnya terbatas pada kelompok pengguna yang memiliki latar belakang teknologi atau yang pernah terlibat dalam pelatihan keamanan siber.[18] Analisis literatur menunjukkan bahwa sebagian besar masyarakat hanya menggunakan internet untuk aktivitas harian tanpa benar-benar memahami bagaimana data mereka diproses atau disimpan oleh layanan digital.

Temuan dari berbagai jurnal internasional menunjukkan bahwa banyak pengguna tidak menyadari ancaman teknis seperti *tracking*, *profiling*, pencurian identitas, atau penyadapan lalu lintas data. Dalam konteks penelitian kepustakaan, peneliti dapat melihat pola berulang dari berbagai literatur bahwa pengguna cenderung menganggap aktivitas digital tidak berbahaya selama mereka tidak melakukan hal-hal yang dianggap "sensitif".[19] Pandangan ini bertentangan dengan temuan penelitian keamanan yang menunjukkan bahwa serangan terhadap pengguna biasa jauh lebih banyak terjadi dibandingkan serangan terhadap target besar, karena pengguna individu umumnya memiliki pertahanan yang jauh lebih lemah.

Literatur lainnya juga menyoroti adanya kecenderungan masyarakat untuk menyepelekan perlindungan data karena mereka merasa tidak memiliki informasi penting yang layak dicuri. Pendekatan analitis dari penelitian sebelumnya menunjukkan bahwa pemahaman yang keliru ini berasal dari kurangnya pengetahuan mengenai bagaimana data dapat dimanfaatkan lebih jauh oleh pihak luar. Data sederhana seperti lokasi, kebiasaan penggunaan aplikasi, atau informasi login dapat digunakan oleh pihak lain untuk menciptakan profil detail seorang individu. Kesadaran mengenai hal ini masih sangat rendah, sebagaimana disebutkan dalam berbagai laporan lembaga keamanan digital internasional.

Melalui pendekatan komparatif dalam library research, ditemukan bahwa tingkat pemahaman masyarakat sangat dipengaruhi oleh latar belakang pendidikan, lingkungan sosial, serta frekuensi paparan informasi mengenai keamanan digital. Di negara-negara yang memiliki budaya literasi digital tinggi, tingkat penggunaan teknologi perlindungan data jauh lebih besar, sedangkan di daerah dengan tingkat literasi rendah, penggunaan perlindungan tambahan hampir tidak

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 2357-2366
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.728

terlihat. Temuan ini memperlihatkan bahwa pengetahuan merupakan faktor yang sangat menentukan dalam adopsi teknologi keamanan.

Selain itu, beberapa literatur menguraikan bahwa kurangnya pemahaman masyarakat sering kali diperparah oleh faktor psikologis. Banyak pengguna merasa bahwa aturan atau langkah keamanan tambahan hanya memperlambat aktivitas mereka, sehingga mereka cenderung mengabaikannya demi kenyamanan. Sumber-sumber psikologi teknologi menunjukkan bahwa manusia memiliki kecenderungan kuat untuk memilih kenyamanan jangka pendek dibandingkan keamanan jangka panjang, terutama ketika ancaman tersebut tidak terlihat secara langsung. Prinsip ini dikenal sebagai *security fatigue*, yaitu kondisi di mana pengguna merasa lelah atau terbebani oleh informasi dan langkah keamanan sehingga memilih untuk tidak melakukannya sama sekali.

Tinjauan literatur juga menunjukkan bahwa program edukasi mengenai keamanan digital masih belum merata. Sebagian besar program tersebut hanya menyasar instansi tertentu, perusahaan, atau individu yang memang bekerja dalam bidang teknologi. Sementara itu, masyarakat umum jarang mendapatkan edukasi yang terstruktur. Banyak peneliti menyebutkan bahwa tidak adanya kurikulum formal terkait literasi digital di berbagai jenjang pendidikan turut berkontribusi pada rendahnya kesadaran mengenai pentingnya menjaga privasi data.

Dalam sintesis teoritis yang dilakukan melalui penelitian kepustakaan, terlihat bahwa rendahnya tingkat pemahaman masyarakat turut mempengaruhi rendahnya adopsi teknologi keamanan digital secara keseluruhan. Walaupun banyak alat perlindungan tersedia baik yang sederhana maupun yang canggih kesadaran pengguna menjadi faktor yang menentukan apakah alat tersebut akan digunakan atau diabaikan. Berbagai literatur menggarisbawahi bahwa teknologi keamanan tidak akan memberikan hasil optimal apabila pengguna tidak mengetahui manfaatnya atau tidak termotivasi untuk menggunakannya.

Dengan demikian, pembahasan ini menunjukkan bahwa minimnya pemahaman masyarakat bukan hanya sekadar persoalan kurangnya informasi, tetapi juga melibatkan faktor sosial, psikologis, dan struktural. Melalui pendekatan library research, persoalan ini dapat dilihat secara menyeluruh dengan membandingkan berbagai penelitian terdahulu yang konsisten menyimpulkan bahwa literasi digital merupakan komponen utama dalam menjaga keamanan dan privasi data di era modern. Pemahaman yang minim ini pada akhirnya menjadi alasan kuat mengapa diperlukan penelitian yang memberikan penjelasan lebih komprehensif mengenai teknologi yang dapat membantu pengguna melindungi aktivitas mereka di dunia digital.

3.4 Analisis Hasil Penelitian

Analisis hasil penelitian ini dilakukan dengan menelaah, mengintegrasikan, dan membandingkan berbagai temuan dari literatur terdahulu yang relevan dengan isu keamanan data dan perlindungan privasi digital. Sebagai penelitian kepustakaan, seluruh kesimpulan dan penilaian didasarkan pada sintesis teori, kajian ilmiah, laporan lembaga keamanan siber, serta penelitian akademik yang telah diterbitkan sebelumnya. Dari keseluruhan literatur yang dianalisis, terdapat sejumlah pola penting yang menguatkan pemahaman mengenai tingkat kerentanan pengguna dan minimnya literasi keamanan digital di masyarakat.

Hasil analisis menunjukkan bahwa kerentanan pengguna pada jaringan publik merupakan salah satu temuan paling konsisten dalam hampir seluruh literatur keamanan siber. Banyak penelitian menggambarkan bahwa jaringan publik, seperti Wi-Fi gratis di area komersial maupun fasilitas umum, dibangun tanpa sistem perlindungan yang memadai. Ketidakhadiran enkripsi dasar membuat setiap data yang dikirimkan pengguna dapat melintas dalam bentuk yang mudah dibaca oleh pihak lain. Literatur teknis khususnya menegaskan bahwa struktur jaringan terbuka tidak memiliki mekanisme otentikasi yang kuat, sehingga siapa pun dapat terhubung ke jaringan tersebut tanpa verifikasi identitas. Hal ini menjadikan jaringan publik bukan hanya rawan disusupi, tetapi secara desain memang tidak ditujukan untuk komunikasi yang bersifat sensitif.[3]

Lebih jauh lagi, berbagai sumber akademik dan laporan lembaga keamanan siber memaparkan bahwa ancaman pada jaringan publik bukan sekadar potensi, melainkan kenyataan yang sering terjadi. Teknik seperti *packet sniffing*, *session hijacking*, hingga *man-in-the-middle attack* disebutkan sebagai metode yang paling sering digunakan untuk menyadap lalu lintas data pada jaringan terbuka. Penyerang dapat dengan mudah memantau apa yang dilakukan pengguna, mulai dari aktivitas sederhana seperti membuka situs web hingga tindakan yang lebih sensitif seperti login ke akun pribadi. Fakta ini diperkuat oleh banyak hasil penyelidikan keamanan yang melaporkan meningkatnya kasus pencurian data pada area yang menyediakan akses internet gratis tanpa perlindungan. Oleh karena itu, dalam perspektif literatur, jaringan publik sering digambarkan sebagai "zona merah" atau wilayah paling berisiko dalam ekosistem komunikasi digital.[4]

Analisis sintesis dari berbagai literatur memperjelas bahwa kerentanan jaringan publik bukanlah peristiwa khusus atau terkait situasi tertentu, melainkan sebuah karakteristik inheren dari sistem jaringan terbuka. Karena tidak adanya kontrol akses, tidak adanya enkripsi kuat, dan tidak adanya mekanisme proteksi tambahan, ancaman terhadap pengguna menjadi melekat pada desain jaringan tersebut. Hal ini berarti bahwa selama jaringan publik tetap dibangun tanpa lapisan keamanan yang memadai, maka risiko intersepsi data akan tetap ada, terlepas dari perangkat atau aplikasi

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 2357-2366
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.728

yang digunakan pengguna. Dari sudut pandang penelitian, hal ini menegaskan bahwa pengguna membutuhkan perlindungan eksternal dan kesadaran yang lebih tinggi agar tidak menyalahartikan kenyamanan akses gratis sebagai jaminan keamanan.[5] Dengan demikian, literatur secara konsisten memberikan gambaran bahwa permasalahan ini merupakan isu struktural yang membutuhkan perhatian serius.

Analisis lebih lanjut juga menunjukkan bahwa serangan pada jaringan publik sering kali tidak disadari oleh korban. Literatur psikologi keamanan menunjukkan bahwa serangan tanpa gejala visual atau fisik membuat pengguna salah menilai tingkat risiko. Dari sinilah muncul kesimpulan analitis bahwa kerentanan jaringan publik tidak hanya berasal dari kelemahan teknis, tetapi juga dari keterbatasan persepsi pengguna terhadap ancaman yang tidak terlihat. Hal ini memperkuat argumentasi bahwa perlindungan tambahan sangat dibutuhkan pada setiap koneksi jaringan yang berpotensi terbuka.

Sementara itu, analisis terhadap minimnya pemahaman masyarakat mengenai perlindungan privasi digital menunjukkan masalah yang lebih kompleks dan multidimensional. Dari berbagai literatur akademik terlihat bahwa tingkat literasi digital masyarakat sangat beragam dan dipengaruhi oleh pendidikan, pengalaman, akses informasi, serta lingkungan sosial. Namun, sebagian besar penduduk digital ternyata tidak memiliki pemahaman mendasar mengenai bagaimana data pribadi mereka diproses, disimpan, atau disebarkan dalam ruang digital. Banyak penelitian internasional menilai masyarakat cenderung menyepelekan ancaman karena merasa tidak memiliki informasi penting atau karena menganggap risiko keamanan adalah urusan penyedia layanan, bukan pengguna.

Analisis literatur juga memperlihatkan bahwa masyarakat memiliki kecenderungan untuk mengutamakan kenyamanan daripada keamanan. Fenomena ini dikenal sebagai *security-comfort trade-off*. Banyak penelitian psikologi teknologi menyebutkan bahwa pengguna sering kali menghindari langkah pengamanan tambahan karena dianggap repetitif, mengganggu alur kerja, atau terasa terlalu teknis. Dengan demikian, rendahnya tingkat adopsi teknologi perlindungan data bukan disebabkan oleh ketiadaan alat, tetapi oleh persepsi bahwa alat-alat tersebut merepotkan atau tidak diperlukan dalam kehidupan sehari-hari.[6]

Dari analisis komparatif antara berbagai literatur, jelas bahwa meskipun teknologi perlindungan data semakin berkembang, pemanfaatannya tidak sebanding dengan kebutuhan. Ketidakseimbangan antara kompleksitas ancaman dan rendahnya pemahaman pengguna membuat ruang digital menjadi semakin rentan. Literatur konsisten menunjukkan bahwa perlindungan data tidak hanya bergantung pada teknologi yang tersedia, tetapi juga pada sejauh mana pengguna memahami dan menggunakannya. Oleh karena itu, solusi teknis apa pun akan kurang efektif apabila tidak diiringi dengan peningkatan literasi digital.

Berdasarkan keseluruhan analisis, dapat disimpulkan bahwa kedua permasalahan utama—kerentanan jaringan publik dan rendahnya literasi pengguna saling berkaitan erat. Kerentanan teknis memperbesar risiko kehilangan data, sementara kurangnya pemahaman memperburuk kemampuan pengguna untuk mengantisipasi risiko tersebut. Dengan demikian, analisis hasil penelitian menegaskan bahwa perlindungan privasi digital membutuhkan pendekatan yang tidak hanya berfokus pada teknologi, tetapi juga pada edukasi dan peningkatan pemahaman masyarakat. Temuan ini menjadi dasar penting untuk merumuskan rekomendasi dan solusi yang relevan dalam pembahasan selanjutnya.

4. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan melalui pendekatan riset perpustakaan, dapat disimpulkan bahwa Virtual Private Network (VPN) memainkan peran penting sebagai alat untuk menjaga keamanan data dan melindungi privasi digital, terutama bagi pengguna yang terhubung ke jaringan publik yang berisiko tinggi terhadap penyadapan serta kebocoran informasi. Sintesis literatur menunjukkan bahwa penggunaan VPN dapat memberikan perlindungan tambahan melalui metode enkripsi dan tunneling, sehingga secara konseptual efektif dalam mengurangi risiko data tertangkap oleh pihak ketiga tanpa mengurangi kepuasan pengguna, yang sesuai dengan tujuan penelitian untuk menganalisis peran VPN dalam meningkatkan keamanan dan privasi digital. Kontribusi ilmiah dari penelitian ini terdapat pada penyampaian pemahaman yang lengkap, yang menggabungkan aspek teknis dari VPN dengan faktor literasi digital pengguna, sehingga memperkaya studi tentang keamanan data yang sebelumnya umumnya hanya fokus pada sisi teknologi saja. Secara praktis, hasil penelitian ini menunjukkan bahwa penggunaanVPN dapat direkomendasikan sebagai solusi keamanan yang relatif mudah diimplementasikan oleh masyarakat umum. Secara teoretis, penelitian ini menekankan pentingnya pendekatan holistik yang menggabungkan penggunaan teknologi serta pendidikan dalam upaya melindungi data. Namun, penelitian ini memiliki keterbatasan karena hanya berupa kajian literatur dan belum menggunakan data empiris atau melakukan uji langsung terhadap penerapanVPN di lapangan. Oleh karena itu, disarankan untuk melakukan penelitian lebih lanjut berupa studi empiris atau eksperimen teknis agar dapat mengukur secara kuantitatif efektivitas penggunaan VPN, membandingkan berbagai jenis protokol yang digunakan, serta menganalisis dampak penggunaan VPN terhadap perilaku dan kesadaran akan keamanan digital pengguna.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 2357-2366
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.728

REFERENCES

[1] N. S. Dinarti, S. R. Salsabila, and Y. T. Herlambang, "Dilema Etika dan Moral dalam Era Digital: Pendekatan Aksiologi Teknologi terhadap Privasi Keamanan, dan Kejahatan Siber," *Daya Nas. J. Pendidik. Ilmu-Ilmu Sos. Dan Hum.*, vol. 2, no. 1, pp. 8–16, 2024.

[2] A. R. Amalia, A. Aqida, and S. Aidah, "Kewarganegaraan Digital Sebagai Upaya Persiapan Menghadapi Tantangan Perkembangan Teknologi," *Indones. Character J.*, vol. 2, no. 1, 2025.

[3] S. Gea, Y. Siregar, and D. Robiyanti, "Pemahaman Masyarakat Terhadap Tantangan Hukum Di Era Media Sosial Tentang Hak Digital Dan Kontroversi Privasi," *J. Dunia Pendidik.*, vol. 5, no. 6, pp. 2507–2524, 2025.

[4] D. Pramono, "Implementasi VPN Menggunakan Mikrotik Untuk Peningkatan Keamanan Jaringan di Bank Syariah Indonesia KCP Jakarta Tanjung Duren 1".

[5] A. S. Wahyusesa, P. W. Hidayanto, and E. A. Ramdayani, "Solusi Cerdas: Meningkatkan Keamanan dan Kinerja Jaringan pada Warnet dengan Mengatasi Kelemahan Sistem," *DIKE J. Ilmu Multidisiplin*, vol. 1, no. 2, pp. 62–66, 2023, doi: 10.69688/dike.v1i2.39.

[6] Zumhur Alamin and Muhammad Amirul Mu'min, "Analisis Keamanan Jaringan pada Sistem Kendali Jarak Jauh untuk Infrastruktur Kritis," *J. Pengemb. Sains dan Teknol.*, vol. 1, no. 1, pp. 25–41, 2025, doi: 10.63866/jpst.v1i1.39.

[7] S. T. Zahwani and M. I. P. Nasution, "Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi di Era Digital," *J. Sharia Econ. Sch.*, vol. 2, no. 2, 2024.

[8] J. Manurung, A. P. E. Sihombing, and B. Pandiangan, "Sosialisasi Dan Edukasi Tentang Keamanan Data Dan Privasi Di Era Digital Untuk Meningkatkan Kesadaran Dan Perlindungan Masyarakat," *J. Pengabdi. Masy. Nauli*, vol. 2, no. 1, pp. 1–7, 2023.

[9] H. S. Disemadi, L. Sudirman, J. Girsang, and A. M. Aninda, "Perlindungan Data Pribadi di Era Digital: Mengapa Kita Perlu Peduli?," *Sang Sewagati J.*, vol. 1, no. 2, pp. 66–90, 2023.

[10] C. A. Zulaeka and R. A. Prastyanti, "PERLINDUNGAN DATA PRIBADI SEBAGAI HAK ASASI: IMPLIKASI SOSIAL DAN ETIS DI TENGAH GLOBALISASI MODERN," *J. Kaji. Huk. Progresif*, vol. 8, no. 2, 2025.

[11] A. Erikha and Z. A. Hoesein, "Strategi pencegahan kebocoran data pribadi melalui peran Kominfo dan gerakan Siberkreasi dalam edukasi digital," *J. Retentum*, vol. 4, no. 1, pp. 48–64, 2025.

[12] R. Firmansyah, "PERAN IT ETHICS AND REGULATION DALAM MENINGKATKAN EFEKTIVITAS CYBERSECURITY DI ERA TEKNOLOGI," *J. Inform. Kaputama*, vol. 9, no. 2, pp. 55–68, 2025.

[13] C. Jerendi, F. Ayu, R. Nasution, and S. P. Sitorus, "KECERDASAN TEKNOLOGI BIG DATA DALAM TRANSFORMASI DIGITAL," *buku*, p. 85, 2026.

[14] S. Gunawan, A. A. R. Santosa, and E. M. S. Sakti, "Analisis Keamanan Jaringan 5G: Ancaman dan Upaya Mitigasi," *J. Ilm. Tek. Inform.*, vol. 25, no. 2, pp. 54–62, 2024.

[15] M. Wali, S. Syafrizal, S. Syafrinal, and F. Fathurrahmad, "Implementasi Signal Protocol untuk meningkatkan keamanan dan kinerja aplikasi Wallchat," *J. Teknol. dan Otomasi*, vol. 1, no. 1, pp. 1–17, 2024.

[16] S. Dewi, "Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point To Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis," *EVOLUSI J. Sains dan Manaj.*, vol. 8, no. 1, pp. 128–139, 2020, doi: 10.31294/evolusi.v8i1.7658.

[17] S. Hakim, R. & Putri, *Keamanan Siber dan Forensik Digital*, no. July. 2023.

[18] K. Syafuddin, Jamalullail, and Rafi'i, "Peningkatan Literasi Keamanan Digital Dan Perlindungan Data Pribadi Bagi Siswa Di Smpn 154 Jakarta," *Eastasouth J. Impactive Community Serv.*, vol. 1, no. 03, pp. 122–133, 2023, doi: 10.58812/ejimcs.v1i03.119.

[19] A. M.R. and V. P., "Review of Cyber Attack Detection: Honeypot System," *Webology*, vol. 19, no. 1, pp. 5497–5514, 2022, doi: 10.14704/web/v19i1/web19370.