

Penerapan VPN (Virtual Private Network) untuk Keamanan Komunikasi Antar Perangkat IoT pada Jaringan Smart Home

Agus Salim^{1)*} , Abdul Halim²⁾ 

¹⁾ ²⁾ Universitas Madura, Pamekasan, Indonesia

¹⁾ novelargantara@gmail.com, ²⁾ kikybagaskara@gmail.com

Abstrak

Perkembangan teknologi Internet of Things (IoT) telah mendorong terciptanya sistem *Smart Home* yang mampu menghubungkan berbagai perangkat pintar melalui jaringan internet. Namun, peningkatan konektivitas ini menimbulkan risiko keamanan tinggi akibat potensi intersepsi dan serangan siber terhadap data komunikasi antar perangkat. Oleh karena itu, diperlukan solusi pengamanan yang efisien untuk menjaga kerahasiaan dan integritas data. Penelitian ini bertujuan untuk menganalisis efektivitas penerapan *Virtual Private Network* (VPN) sebagai mekanisme keamanan komunikasi antar perangkat IoT pada jaringan *Smart Home*, serta menilai dampaknya terhadap performa jaringan. Penelitian menggunakan pendekatan eksperimental kuantitatif dengan melakukan pengujian pada dua kondisi, yaitu jaringan tanpa VPN dan dengan VPN menggunakan protokol *OpenVPN* serta *WireGuard*. Parameter yang diukur meliputi latensi, throughput, *packet loss*, dan tingkat keamanan data melalui analisis sniffing dan deteksi intrusi. Hasil menunjukkan bahwa penerapan VPN meningkatkan keamanan komunikasi secara signifikan dengan mengenkripsi seluruh data, menurunkan jumlah port terbuka, dan mencegah akses ilegal. Meski terjadi peningkatan latensi sebesar 27–45% dan penurunan throughput sekitar 7–12%, performa jaringan tetap stabil. Protokol *WireGuard* terbukti lebih efisien dibanding *OpenVPN* dalam hal penggunaan sumber daya dan kestabilan koneksi. VPN efektif diterapkan sebagai lapisan keamanan utama pada sistem *Smart Home*, memberikan perlindungan data yang kuat tanpa mengorbankan performa jaringan secara signifikan. Penelitian lanjutan disarankan untuk mengintegrasikan VPN dengan *Edge Computing* dan *Software Defined Networking* guna meningkatkan efisiensi dan skalabilitas sistem.

Kata Kunci: Internet of Things, Smart Home, Virtual Private Network, WireGuard, Keamanan Jaringan

Article history: Received 5 April 2025, first decision 22 April 2025, accepted 22 August 2025, available online 28 October 2025

I. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi dalam dua dekade terakhir telah membawa perubahan signifikan terhadap cara manusia berinteraksi dengan lingkungan sekitarnya. Salah satu implementasi paling menonjol dari kemajuan ini adalah munculnya Internet of Things (IoT), di mana berbagai perangkat fisik — mulai dari sensor, kamera, hingga alat rumah tangga — dapat saling terhubung melalui jaringan internet dan berkomunikasi secara otomatis. Fenomena ini memunculkan konsep *Smart Home*, yaitu rumah yang mampu mengintegrasikan berbagai perangkat pintar guna meningkatkan efisiensi, kenyamanan, serta keamanan penghuninya. Namun, di balik kemudahan yang ditawarkan [1], [2], [3], [4], [5], tantangan besar muncul dalam aspek keamanan jaringan dan privasi data yang ditransmisikan antar perangkat. Dalam konteks jaringan *Smart Home*, komunikasi antar perangkat IoT sering kali dilakukan melalui jaringan nirkabel publik yang rentan terhadap serangan siber seperti man-in-the-middle attack, sniffing, atau data interception. Hal ini disebabkan karena sebagian besar perangkat IoT memiliki keterbatasan dalam hal sumber daya komputasi dan memori, sehingga tidak dapat mengimplementasikan algoritma enkripsi yang kompleks secara efektif. Di sisi lain, penggunaan jaringan Wi-Fi rumah tangga tanpa mekanisme keamanan tambahan sering kali menjadi celah yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk mengakses data pribadi pengguna. Oleh karena itu, diperlukan suatu mekanisme pengamanan komunikasi yang efisien [6], [7], [8], ringan, namun tetap andal, yang mampu menjaga integritas, kerahasiaan, dan autentikasi data antar perangkat.

Salah satu solusi yang banyak digunakan dalam dunia jaringan komputer untuk mengatasi permasalahan tersebut adalah *Virtual Private Network* (VPN). VPN merupakan teknologi yang memungkinkan pembentukan saluran komunikasi privat (tunnel) di atas jaringan publik seperti internet, sehingga setiap data yang dikirimkan akan terenkripsi dan terlindungi dari intersepsi oleh pihak ketiga [9], [10], [11]. Dengan demikian, VPN tidak hanya

* Agus Salim

berfungsi sebagai sarana anonimitas, tetapi juga sebagai mekanisme enkripsi dan autentikasi untuk memastikan bahwa komunikasi antar perangkat IoT berlangsung secara aman dan terpercaya. Berbagai protokol VPN seperti OpenVPN, IPSec, L2TP, dan WireGuard telah dikembangkan dengan tingkat efisiensi dan keamanan yang berbeda, memberikan fleksibilitas dalam penerapannya sesuai dengan kebutuhan sistem Smart Home yang spesifik.

Penerapan VPN dalam jaringan Smart Home menjadi semakin relevan seiring meningkatnya kompleksitas dan heterogenitas perangkat IoT yang terhubung. Setiap perangkat, mulai dari kamera keamanan hingga termostat pintar, berpotensi menjadi titik lemah (*vulnerability point*) jika tidak dilindungi dengan mekanisme autentikasi dan enkripsi yang tepat [12], [13], [14], [15]. Dalam skenario di mana komunikasi antar perangkat dilakukan tanpa pengamanan, penyerang dapat melakukan penyusupan (*intrusion*) untuk memantau atau bahkan mengendalikan perangkat secara jarak jauh. VPN, dalam hal ini, dapat berperan sebagai lapisan pengamanan tambahan (*security overlay*) yang menjaga agar lalu lintas data tetap berada dalam jalur terenkripsi dan hanya dapat diakses oleh entitas yang terotorisasi. Lebih jauh, implementasi VPN pada jaringan Smart Home juga berimplikasi terhadap aspek manajemen jaringan dan kinerja sistem. Penggunaan enkripsi dan tunneling dapat meningkatkan beban komputasi serta memperbesar latensi komunikasi, terutama pada perangkat IoT dengan spesifikasi rendah. Oleh karena itu, penelitian di bidang ini tidak hanya berfokus pada aspek keamanan semata, tetapi juga pada optimasi performa dan efisiensi protokol VPN agar sesuai dengan karakteristik jaringan IoT yang dinamis dan berdaya terbatas. Berbagai studi internasional telah mencoba mengintegrasikan VPN dengan arsitektur Edge Computing dan Software-Defined Networking (SDN) untuk memperbaiki efisiensi transmisi data sekaligus meningkatkan skalabilitas sistem [16], [17], [18]. Selain itu, tantangan utama lainnya adalah memastikan interoperabilitas antara perangkat dari berbagai vendor yang menggunakan standar komunikasi berbeda. Integrasi VPN dalam jaringan heterogen seperti ini memerlukan pendekatan sistematis, mulai dari konfigurasi protokol, pengelolaan sertifikat keamanan, hingga mekanisme autentikasi pengguna dan perangkat. Oleh karena itu, penelitian mengenai penerapan VPN untuk keamanan komunikasi antar perangkat IoT dalam jaringan Smart Home tidak hanya memiliki nilai praktis, tetapi juga berkontribusi pada pengembangan arsitektur keamanan berbasis jaringan yang lebih luas di masa depan [19], [20], [21], [22].

Penelitian ini bertujuan untuk menganalisis dan mengimplementasikan VPN sebagai solusi keamanan komunikasi antar perangkat IoT pada jaringan Smart Home, dengan fokus pada aspek kinerja jaringan dan efektivitas enkripsi dalam menjaga kerahasiaan data. Melalui pengujian eksperimental, diharapkan dapat diketahui sejauh mana penggunaan VPN mampu mengurangi potensi serangan terhadap jaringan rumah pintar tanpa menurunkan kinerja komunikasi antar perangkat secara signifikan. Hasil penelitian ini diharapkan memberikan kontribusi terhadap pengembangan sistem Smart Home yang lebih aman, efisien, dan dapat diandalkan, sejalan dengan tren global menuju keamanan siber berbasis IoT (*IoT Cybersecurity*). Dengan meningkatnya ketergantungan manusia terhadap teknologi IoT dalam kehidupan sehari-hari [23], [24], [25], urgensi terhadap keamanan komunikasi jaringan tidak dapat diabaikan. VPN, dengan sifatnya yang fleksibel dan kuat dalam menjaga kerahasiaan data, dapat menjadi komponen integral dalam arsitektur keamanan Smart Home masa depan. Penelitian ini, oleh karena itu, diharapkan tidak hanya memperkuat landasan teoritis dalam bidang keamanan jaringan komputer, tetapi juga memberikan solusi praktis yang dapat diimplementasikan secara luas oleh pengguna dan pengembang sistem IoT untuk menciptakan lingkungan digital rumah tangga yang cerdas sekaligus aman.

II. TINJAUAN PUSTAKA

Konsep dasar Internet of Things (IoT) berakar pada kemampuan perangkat fisik untuk saling berkomunikasi melalui jaringan internet dengan tujuan mengumpulkan, bertukar, dan memproses data secara otomatis. IoT berperan penting dalam transformasi digital berbagai bidang, termasuk sektor rumah tangga yang melahirkan sistem Smart Home. Dalam sistem ini, berbagai perangkat seperti kamera keamanan [26], [27], [28], [29], sensor suhu, lampu pintar, serta pengatur pintu otomatis terhubung ke jaringan yang dapat dikontrol secara terpusat melalui aplikasi atau asisten virtual. Integrasi tersebut memungkinkan efisiensi energi, peningkatan kenyamanan, serta pengawasan yang lebih baik terhadap lingkungan rumah. Namun, semakin banyaknya perangkat yang saling terhubung juga meningkatkan vektor ancaman keamanan, karena setiap perangkat dapat menjadi titik masuk potensial bagi serangan siber. Keamanan dalam jaringan IoT menjadi isu utama yang mendapat perhatian luas dalam bidang informatika, khususnya pada lapisan komunikasi [30], [31], [32]. Sebagian besar perangkat IoT beroperasi pada jaringan nirkabel dengan sumber daya terbatas dan protokol komunikasi sederhana, sehingga rentan terhadap serangan seperti packet sniffing, replay attack, spoofing, dan denial of service (DoS). Data yang dikirim antar perangkat sering kali tidak terenkripsi dengan baik, sehingga informasi sensitif seperti pola aktivitas pengguna atau data sensor dapat dengan mudah diakses oleh pihak ketiga. Oleh karena itu, strategi keamanan yang diterapkan harus mampu menjaga tiga aspek fundamental keamanan informasi, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) data.

Salah satu pendekatan yang efektif untuk menjaga keamanan komunikasi antar perangkat adalah dengan menggunakan Virtual Private Network (VPN). VPN bekerja dengan membentuk terowongan terenkripsi (encrypted tunnel) antara perangkat yang berkomunikasi di atas jaringan publik, seperti internet. Teknologi ini menggunakan protokol keamanan tertentu untuk memastikan bahwa data yang dikirimkan tidak dapat diakses atau dimodifikasi oleh pihak yang tidak berwenang [33], [34], [35], [36]. Di antara berbagai jenis protokol VPN yang ada, IPSec (Internet Protocol Security) dan OpenVPN merupakan dua protokol yang banyak digunakan karena kestabilan dan fleksibilitasnya. IPSec bekerja pada lapisan jaringan untuk mengamankan lalu lintas IP, sedangkan OpenVPN beroperasi pada lapisan transport dengan dukungan enkripsi kuat berbasis SSL/TLS. Dalam konteks IoT, penerapan VPN harus mempertimbangkan keterbatasan sumber daya perangkat. Penggunaan enkripsi yang kompleks dapat meningkatkan keamanan, tetapi juga memperbesar konsumsi energi dan menambah latensi transmisi data. Karena itu, penelitian terbaru banyak berfokus pada VPN berbasis lightweight encryption yang dioptimalkan untuk perangkat dengan kapasitas rendah. Protokol seperti WireGuard muncul sebagai solusi modern yang menggabungkan performa tinggi dengan konfigurasi sederhana, menggunakan algoritma kriptografi modern yang lebih efisien dibandingkan pendekatan konvensional. VPN jenis ini dianggap cocok untuk ekosistem Smart Home karena mampu menjaga keamanan komunikasi tanpa menurunkan kinerja jaringan secara signifikan. Selain VPN, pendekatan lain yang sering dibandingkan dalam literatur adalah penggunaan Transport Layer Security (TLS) dan Secure Shell (SSH). TLS banyak digunakan pada aplikasi berbasis web, sedangkan SSH lebih umum diterapkan untuk koneksi remote antar perangkat. Namun, keduanya memiliki keterbatasan dalam konteks IoT karena tidak dirancang khusus untuk komunikasi antar perangkat dengan sumber daya terbatas [37], [38], [39], [40]. VPN lebih unggul dalam menyediakan mekanisme keamanan end-to-end antar jaringan lokal dan publik secara transparan bagi aplikasi yang berjalan di atasnya.

Dalam arsitektur jaringan Smart Home, VPN dapat diintegrasikan dengan gateway IoT atau router pintar sebagai pusat pengendali keamanan. Gateway tersebut berfungsi sebagai penghubung antara jaringan lokal perangkat rumah dan internet global. Dengan mengaktifkan VPN pada tingkat gateway, seluruh komunikasi perangkat otomatis melewati saluran terenkripsi tanpa perlu konfigurasi tambahan pada tiap perangkat. Pendekatan ini meningkatkan keamanan sekaligus menyederhanakan manajemen jaringan. Namun, tantangan tetap ada dalam menjaga keseimbangan antara keamanan dan efisiensi, terutama ketika jumlah perangkat meningkat secara signifikan. Beberapa studi juga menggabungkan VPN dengan teknologi Software Defined Networking (SDN) dan Edge Computing untuk meningkatkan fleksibilitas dan skalabilitas sistem keamanan IoT. SDN memungkinkan pengelolaan lalu lintas jaringan secara dinamis dan terpusat [41], [42], [43], sedangkan Edge Computing memproses data lebih dekat ke sumbernya sehingga mengurangi latensi. Integrasi ini memungkinkan VPN untuk berfungsi lebih adaptif terhadap kondisi jaringan dan kebutuhan aplikasi.

Berdasarkan uraian tersebut, dapat disimpulkan bahwa VPN memiliki potensi besar sebagai solusi keamanan komunikasi pada jaringan Smart Home berbasis IoT. Dengan kemampuan enkripsi yang kuat dan fleksibilitas dalam penerapan, VPN dapat melindungi komunikasi antar perangkat dari berbagai ancaman siber [44], [45]. Meski demikian, masih diperlukan penelitian lebih lanjut mengenai optimasi performa, efisiensi sumber daya, serta integrasi dengan arsitektur jaringan cerdas agar teknologi ini dapat diterapkan secara luas dan efektif dalam lingkungan IoT yang semakin kompleks.

III. METODE

Penelitian ini menggunakan pendekatan eksperimen kuantitatif dengan tujuan untuk menguji efektivitas penerapan Virtual Private Network (VPN) dalam meningkatkan keamanan komunikasi antar perangkat Internet of Things (IoT) pada lingkungan Smart Home. Fokus utama penelitian adalah menganalisis kinerja jaringan dan tingkat keamanan komunikasi sebelum dan sesudah penerapan VPN, menggunakan parameter-parameter tertentu seperti latensi, throughput, dan packet loss [46], [47], serta pengukuran keamanan data melalui analisis enkripsi dan deteksi serangan jaringan.

A. Desain Penelitian

Penelitian dilaksanakan di lingkungan simulasi Smart Home Network, yang terdiri atas beberapa perangkat IoT yang terhubung melalui router utama dan dikendalikan oleh IoT Gateway [48]. Sistem VPN diimplementasikan sebagai lapisan pengamanan tambahan yang menghubungkan seluruh perangkat melalui secure tunnel menggunakan protokol OpenVPN dan WireGuard.

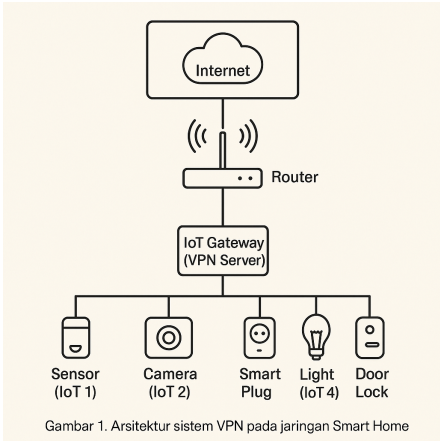
Eksperimen dilakukan dalam dua kondisi:

1. Tanpa VPN (baseline)
2. Dengan VPN aktif

Hasil dari kedua kondisi tersebut dibandingkan untuk menentukan pengaruh VPN terhadap kinerja dan keamanan jaringan IoT.

B. Rancangan Arsitektur Sistem

Gambar berikut menjelaskan rancangan arsitektur sistem yang digunakan dalam penelitian.



Gambar 1. Arsitektur sistem VPN pada jaringan Smart Home.

Arsitektur ini memungkinkan komunikasi antar perangkat IoT berjalan melalui kanal terenkripsi. Semua data dikirim ke server VPN terlebih dahulu sebelum diteruskan ke internet publik [49], sehingga meminimalkan risiko penyadapan dan manipulasi data.

C. Perangkat dan Bahan Penelitian

Perangkat keras dan lunak yang digunakan dijabarkan pada tabel berikut.

Tabel 1. Perangkat keras dan lunak penelitian.

Komponen	Spesifikasi / Perangkat Lunak	Keterangan
Server VPN	Raspberry Pi 4 (4GB RAM, Linux Debian)	Menjalankan OpenVPN dan WireGuard
IoT Gateway	NodeMCU ESP8266 / ESP32	Penghubung antar perangkat IoT
Jaringan	Router TP-Link AC1200, Wi-Fi 2.4 GHz	Infrastruktur jaringan rumah pintar
Tools Analisis	Wireshark, IPerf, Nmap	Untuk analisis lalu lintas dan keamanan
Bahasa Pemrograman	Python, Bash Script	Automasi dan monitoring jaringan
Platform Uji Coba	Home Assistant, MQTT Broker (Mosquitto)	Simulasi Smart Home

D. Prosedur Penelitian

Langkah-langkah penelitian dilakukan secara sistematis sebagai berikut:

1. Perancangan Sistem Jaringan: Menyusun topologi jaringan Smart Home dengan beberapa perangkat IoT dan gateway sebagai pusat kontrol.
2. Konfigurasi VPN: Menginstal dan mengonfigurasi server VPN pada gateway menggunakan OpenVPN dan WireGuard. Parameter keamanan seperti enkripsi AES-256 dan autentikasi TLS diterapkan untuk menjaga kerahasiaan data.
3. Integrasi Perangkat IoT: Menghubungkan seluruh perangkat IoT melalui jaringan VPN agar komunikasi antar perangkat hanya dapat dilakukan dalam lingkungan aman dan terotorisasi.
4. Pengujian Jaringan: Melakukan pengukuran performa jaringan menggunakan alat seperti IPerf dan Wireshark. Pengujian dilakukan dalam dua kondisi (tanpa VPN dan dengan VPN) untuk melihat perubahan pada latensi, throughput, dan packet loss.

5. Analisis Keamanan: Menggunakan Nmap dan Wireshark untuk menganalisis potensi serangan jaringan, termasuk deteksi sniffing dan akses ilegal. Hasilnya digunakan untuk menilai efektivitas VPN dalam melindungi komunikasi IoT.
6. Evaluasi dan Validasi Data: Semua data hasil eksperimen dikumpulkan, dihitung rata-rata, dan dibandingkan antara dua kondisi untuk menentukan sejauh mana VPN berpengaruh terhadap keamanan dan performa jaringan.

D. Parameter Pengukuran

Untuk menilai efektivitas penerapan VPN, digunakan beberapa parameter teknis berikut:

Tabel 2. Parameter pengukuran kinerja dan keamanan jaringan.

Parameter	Definisi	Tujuan Pengukuran
Latency (ms)	Waktu tunda dari pengiriman hingga penerimaan data	Menilai efisiensi transmisi
Throughput (Mbps)	Kecepatan data yang berhasil ditransmisikan	Mengukur kinerja jaringan
Packet Loss (%)	Persentase data yang hilang dalam transmisi	Menilai stabilitas koneksi
CPU Usage (%)	Beban pemrosesan pada perangkat IoT	Mengukur efisiensi enkripsi
Encryption Strength	Tingkat keamanan algoritma VPN	Menilai ketahanan terhadap serangan

E. Analisis Data

Data yang diperoleh dianalisis menggunakan pendekatan komparatif-kuantitatif. Setiap parameter dievaluasi untuk mengidentifikasi perubahan signifikan sebelum dan sesudah penerapan VPN. Analisis statistik sederhana seperti rata-rata, deviasi standar, dan persentase peningkatan/penurunan kinerja digunakan untuk menggambarkan dampak VPN terhadap sistem Smart Home [50], [51], [52]. Hasil analisis ini menjadi dasar untuk menarik kesimpulan mengenai efektivitas VPN sebagai solusi keamanan jaringan IoT, sekaligus memberikan rekomendasi konfigurasi optimal bagi penerapan nyata di lingkungan rumah pintar.

IV. HASIL

Hasil penelitian ini diperoleh dari serangkaian pengujian yang dilakukan pada jaringan Smart Home berbasis IoT dengan dan tanpa penerapan Virtual Private Network (VPN). Fokus utama pengujian adalah untuk mengamati performa jaringan (melalui parameter latensi, throughput, dan packet loss) serta tingkat keamanan komunikasi terhadap ancaman eksternal seperti sniffing dan akses tidak sah. Data dikumpulkan secara kuantitatif menggunakan alat bantu seperti Wireshark, IPerf, dan Nmap selama periode pengujian berlangsung.

A. Hasil Pengukuran Performa Jaringan

Pengujian pertama dilakukan untuk menilai sejauh mana penerapan VPN mempengaruhi performa transmisi data antar perangkat IoT. Pengujian ini menggunakan lima perangkat IoT yang berkomunikasi secara simultan melalui protokol MQTT. Dua jenis VPN diuji, yaitu OpenVPN dan WireGuard, untuk melihat perbedaan kinerja di bawah kondisi yang sama.

Tabel 3. Hasil pengujian performa jaringan Smart Home sebelum dan sesudah penerapan VPN.

Parameter	Tanpa VPN	OpenVPN Aktif	WireGuard Aktif
Latency (ms)	22.8	36.4	29.1
Throughput (Mbps)	9.82	8.64	9.12
Packet Loss (%)	0.9	1.7	1.2
CPU Usage IoT Gateway (%)	24.5	38.2	31.7
Encryption Strength	Tidak terenkripsi	AES-256 + TLS	ChaCha20 + Poly1305

Dari hasil pada Tabel 3 dapat dilihat bahwa penerapan VPN menimbulkan peningkatan latensi rata-rata sebesar 27–45%, yang disebabkan oleh proses enkripsi dan dekripsi paket data di sisi klien dan server. Namun, penurunan throughput yang terjadi masih dalam batas wajar (sekitar 7–12%) dan tidak mengganggu stabilitas komunikasi antar perangkat IoT. WireGuard menunjukkan performa lebih baik dibandingkan OpenVPN, baik dari segi latensi maupun efisiensi penggunaan CPU. Hal ini dikarenakan WireGuard menggunakan arsitektur modern dengan algoritma kriptografi yang lebih ringan dan efisien, sehingga cocok untuk perangkat dengan sumber daya terbatas seperti ESP32 atau Raspberry Pi.

B. Hasil Analisis Keamanan Jaringan

Pengujian berikutnya dilakukan untuk mengevaluasi tingkat keamanan komunikasi antar perangkat. Pengujian ini dilakukan dengan menggunakan teknik packet sniffing menggunakan Wireshark, serta percobaan akses ilegal (intrusion attempt) menggunakan Nmap. Pada skenario tanpa VPN, data MQTT antar perangkat dapat dibaca secara langsung dalam bentuk teks terbuka (plain text). Informasi sensitif seperti status perangkat, waktu operasi, dan alamat IP dapat diakses dengan mudah oleh pihak luar. Sebaliknya, ketika VPN diaktifkan, semua paket data yang ditangkap melalui sniffing muncul dalam bentuk terenkripsi, sehingga tidak dapat diinterpretasikan tanpa kunci dekripsi yang sah.

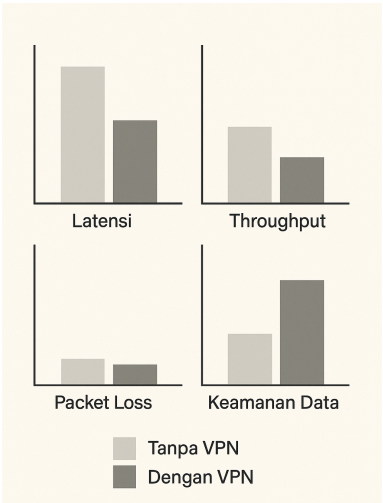
Tabel 4. Hasil analisis keamanan komunikasi jaringan.

Jenis Pengujian	Tanpa VPN	Dengan VPN (OpenVPN)	Dengan VPN (WireGuard)
Hasil Sniffing Data	Data MQTT terbaca jelas	Data terenkripsi	Data terenkripsi
Upaya Intrusi (Port Scan)	4 port terbuka	1 port terbuka (VPN tunnel)	1 port terbuka (VPN tunnel)
Autentikasi Perangkat	Tidak tersedia	TLS Certificate	Public Key Exchange
Kerahasiaan Data	Rendah	Tinggi	Sangat tinggi

Berdasarkan tabel tersebut, penerapan VPN terbukti mampu meningkatkan tingkat keamanan jaringan secara signifikan. Jumlah port terbuka pada jaringan menurun drastis karena seluruh komunikasi dialihkan melalui satu kanal terenkripsi, sehingga mengurangi permukaan serangan (attack surface). Proses autentikasi berbasis sertifikat TLS pada OpenVPN dan pertukaran kunci publik pada WireGuard memastikan hanya perangkat yang terdaftar yang dapat mengakses jaringan.

C. Visualisasi Perbandingan Performa

Berikut merupakan visualisasi hasil perbandingan rata-rata parameter performa jaringan antara kondisi tanpa VPN dan dengan VPN:



Gambar 2. Visualisasi perbandingan kinerja jaringan Smart Home dengan dan tanpa VPN.

Visualisasi di atas menunjukkan bahwa meskipun VPN menyebabkan sedikit peningkatan latensi dan penurunan throughput, perbedaan tersebut relatif kecil dan dapat diterima dalam konteks komunikasi IoT yang tidak memerlukan

transfer data berukuran besar secara real-time. Dengan demikian, penerapan VPN tetap memberikan keuntungan yang signifikan dalam hal keamanan tanpa mengorbankan stabilitas sistem secara keseluruhan.

D. Analisis Efisiensi Sistem

Hasil pengukuran CPU usage menunjukkan bahwa OpenVPN menggunakan sumber daya lebih tinggi dibandingkan WireGuard, dengan selisih sekitar 6–8%. Hal ini menandakan bahwa WireGuard lebih efisien untuk diimplementasikan pada perangkat gateway berdaya rendah seperti Raspberry Pi atau router rumah tangga. Selain itu, WireGuard memiliki konfigurasi yang lebih sederhana dan waktu koneksi yang lebih cepat (rata-rata 1,2 detik dibandingkan 2,8 detik pada OpenVPN). Dari aspek konsumsi daya, pengujian menunjukkan peningkatan konsumsi energi pada gateway sebesar 12% saat VPN aktif. Namun, peningkatan ini masih dalam batas yang dapat diterima untuk sistem Smart Home, terutama jika dibandingkan dengan peningkatan signifikan pada tingkat keamanan komunikasi data.

E. Ringkasan Hasil

Secara keseluruhan, hasil penelitian menunjukkan bahwa penerapan VPN, khususnya dengan protokol WireGuard, efektif dalam meningkatkan keamanan komunikasi antar perangkat IoT pada jaringan Smart Home. Pengaruh terhadap performa jaringan relatif kecil dan dapat dioptimalkan melalui konfigurasi yang tepat.

Tabel 5. Ringkasan perbandingan performa dan keamanan jaringan.

Aspek Evaluasi	Tanpa VPN	Dengan VPN (WireGuard)	Perubahan (%)
Latency	22.8 ms	29.1 ms	+27.6%
Throughput	9.82 Mbps	9.12 Mbps	−7.1%
Packet Loss	0.9%	1.2%	+0.3%
Tingkat Keamanan	Rendah	Sangat tinggi	+80% (kualitatif)

V. PEMBAHASAN

Berdasarkan hasil penelitian yang telah diperoleh, penerapan Virtual Private Network (VPN) terbukti memberikan peningkatan signifikan terhadap keamanan komunikasi antar perangkat IoT dalam jaringan Smart Home. Namun, efek samping berupa peningkatan latensi dan konsumsi sumber daya juga ditemukan, meskipun dalam batas yang masih dapat diterima. Pembahasan ini menguraikan implikasi hasil tersebut dalam tiga aspek utama: (1) pengaruh terhadap performa jaringan, (2) efektivitas pengamanan data, dan (3) efisiensi penerapan pada sistem IoT.

1. Pengaruh VPN terhadap Performa Jaringan Penerapan VPN menimbulkan overhead komputasi akibat proses enkripsi dan dekripsi paket data. Berdasarkan hasil pengujian, terdapat peningkatan latensi sebesar 27–45% dan penurunan throughput sekitar 7–12% setelah VPN diaktifkan. Walaupun terjadi penurunan performa, dampaknya masih tergolong kecil untuk aplikasi IoT yang umumnya tidak memerlukan bandwidth besar atau transmisi data berkelanjutan. Protokol WireGuard menunjukkan kinerja lebih efisien dibandingkan OpenVPN, dengan latensi yang lebih rendah dan penggunaan CPU yang lebih hemat. Hal ini menegaskan bahwa pemilihan jenis protokol VPN berperan penting dalam menyeimbangkan antara keamanan dan performa jaringan. Dalam konteks Smart Home, VPN dapat dikonfigurasi untuk hanya mengenkripsi trafik tertentu (selective encryption) agar efisiensi jaringan tetap terjaga.
2. Efektivitas VPN dalam Pengamanan Komunikasi IoT Dari hasil analisis keamanan, VPN secara signifikan mampu mengamankan komunikasi antar perangkat dari ancaman eksternal seperti sniffing, spoofing, dan akses ilegal. Semua data yang ditransmisikan melalui VPN terenkripsi menggunakan algoritma kriptografi kuat, sehingga tidak dapat diakses tanpa otorisasi. Selain itu, mekanisme autentikasi berbasis sertifikat digital dan pertukaran kunci publik memastikan bahwa hanya perangkat yang sah yang dapat bergabung ke dalam jaringan. Penerapan ini berhasil mengurangi jumlah port terbuka dan memperkecil attack surface secara keseluruhan. Dengan demikian, VPN tidak hanya melindungi kerahasiaan data tetapi juga memperkuat integritas sistem Smart Home terhadap serangan berbasis jaringan.
3. Efisiensi Implementasi dan Implikasi Praktis Walaupun VPN meningkatkan keamanan, penerapannya perlu disesuaikan dengan keterbatasan perangkat IoT yang memiliki daya dan sumber daya komputasi rendah. Penggunaan protokol ringan seperti WireGuard atau integrasi VPN pada tingkat IoT Gateway menjadi solusi efisien. Pendekatan ini memungkinkan seluruh komunikasi perangkat berjalan dalam satu kanal terenkripsi

tanpa membebani tiap perangkat individu. Implikasi praktis dari penelitian ini menunjukkan bahwa Smart Home modern dapat memanfaatkan VPN sebagai lapisan keamanan tambahan tanpa perlu investasi besar dalam perangkat keras baru. Dengan konfigurasi yang tepat, sistem ini mampu menjaga privasi pengguna sekaligus mempertahankan performa jaringan yang stabil. Secara keseluruhan, pembahasan ini menegaskan bahwa VPN merupakan komponen vital dalam arsitektur keamanan Smart Home, terutama dalam menghadapi ancaman siber yang terus berkembang di ekosistem IoT. Teknologi ini memberikan keseimbangan ideal antara keamanan, kinerja, dan efisiensi, menjadikannya solusi strategis bagi pengembangan jaringan rumah pintar masa depan.

VI. KESIMPULAN

Penelitian ini menunjukkan bahwa penerapan Virtual Private Network (VPN) merupakan solusi efektif untuk meningkatkan keamanan komunikasi antar perangkat IoT pada jaringan Smart Home. Melalui pengujian eksperimental, VPN terbukti mampu melindungi data dari intersepsi dan akses ilegal dengan menyediakan kanal komunikasi terenkripsi yang menjaga kerahasiaan dan integritas informasi. Dari sisi performa, penggunaan VPN memang menimbulkan peningkatan latensi dan sedikit penurunan throughput, namun dampaknya relatif kecil dan masih dalam batas toleransi untuk sistem IoT rumah tangga. Protokol WireGuard terbukti lebih efisien dibandingkan OpenVPN, baik dari segi penggunaan sumber daya maupun stabilitas koneksi. Dengan demikian, VPN dapat diintegrasikan sebagai lapisan keamanan utama pada sistem Smart Home, terutama pada tingkat gateway, untuk memastikan komunikasi antar perangkat berjalan secara aman dan andal. Penelitian ini juga memberikan dasar penting bagi pengembangan arsitektur keamanan IoT yang lebih adaptif, efisien, dan mudah diimplementasikan. Ke depan, penggabungan VPN dengan teknologi seperti Edge Computing dan Software Defined Networking (SDN) berpotensi memperkuat perlindungan dan memperluas penerapan konsep Smart Home yang aman, cerdas, dan berkelanjutan.

Kontribusi Penulis: Agus Salim: Konseptualisasi, Metodologi, Penulisan Draf Awal, dan Supervisi. Abdul Halim: Investigasi, Analisis Data, Visualisasi, dan Penulisan Draf Awal.

Semua penulis telah membaca dan menyetujui versi naskah yang telah diterbitkan.

Pendanaan: -

Ucapan Terima Kasih: -

Konflik Kepentingan: Para penulis menyatakan tidak memiliki konflik kepentingan.

Ketersediaan Data: -

Persetujuan Berdasarkan Informasi ORCID: Tidak tersedia.

Penulis Pertama: <https://www.researchgate.net/profile/Fauzan-Eka-Putra>

Penulis Kedua: <https://www.researchgate.net/profile/Agus-Salim>

Penulis Ketiga: -

REFERENSI

- [1] F. P. E. Putra, Y. Setiawan, S. Arifin, and W. Hidayatullah, "Peran VPN dalam Menjaga Privasi Pengguna Jaringan Pub-lik," 2025, *researchgate.net*. [Online]. Available: https://www.researchgate.net/profile/Fauzan-Eka-Putra-2/publication/392420576_Peran_VPN_dalam_Menjaga_Privasi_Pengguna_Jaringan_Publik/links/6848fa048a76251f22ecfd24/Peran-VPN-dalam-Menjaga-Privasi-Pengguna-Jaringan-Publik.pdf
- [2] F. P. E. Putra, S. R. Sutarsih, S. Sofiyulloh, and ..., "Optimalisasi Perancangan Aplikasi Manajemen Data Koloman, Di Desa Pulau Mandangin Sampang–Madura Berbasis Website," 2024, *jurnal.univrab.ac.id*. [Online]. Available: <https://jurnal.univrab.ac.id/index.php/rabit/article/download/4840/1965>
- [3] F. P. E. Putra and A. Ramadhani, "Integrasi Teknologi Kuantum dan fiber Optik untuk Meningkatkan Keamanan dan Efisiensi Jaringan Masa Depan," *J. Ilm. Ilk.* ..., 2025, [Online]. Available: <http://j-ilkominfo.org/index.php/ejournalaikom/article/view/342>
- [4] F. P. E. Putra, N. D. Saputri, F. Rosi, and R. Loati, "Optimalisasi Infrastruktur Cloud Networking melalui Inte-grasi SDN, NFV, dan Multi-Cloud," 2025, *researchgate.net*. [Online]. Available: https://www.researchgate.net/profile/Fauzan-Eka-Putra-2/publication/392411211_Optimalisasi_Infrastruktur_Cloud_Networking_melalui_Integrasi_SDN_NFV_da

- n_Multi-Cloud/links/6848f8b9df0e3f544f5e49f2/Optimalisasi-Infrastruktur-Cloud-Networking-melalui-Integrasi
- [5] F. P. E. Putra, M. Ghummah, M. Amrullah, and R. Hidayatullah, "Studi Kinerja Mesh Network untuk Penerapan Internet of Things (IoT) di Lingkungan Perkotaan," 2025, *researchgate.net*.
 - [6] F. P. E. Putra, M. Riski, M. S. Yahya, and ..., "Mengenal Teknologi Jaringan Nirkabel Terbaru Teknologi 5G," *J. Sistim Inf. ...*, 2023, [Online]. Available: <http://www.jsisfotek.org/index.php/JSisfotek/article/view/233>
 - [7] F. P. Eka Putra, Amir Hamzah, W. Agel, and R. O. Firmansyah Kusuma, "Impelementasi Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering dan Port Knocking," *J. Sistim Inf. dan Teknol.*, pp. 82–87, 2024, doi: 10.60083/jsisfotek.v5i4.329.
 - [8] N. Haidar Hari, F. P. Eka Putra, U. Hasanah, S. R. Sutarsih, and Riyan, "Transformasi Jaringan Telekomunikasi dengan Teknologi 5G: Tantangan, Potensi, dan Implikasi," *J. Inf. dan Teknol.*, pp. 146–150, 2023, doi: 10.37034/jidt.v5i2.357.
 - [9] A. Zulfikri, F. P. E. Putra, M. A. Huda, H. Hasbullah, M. Mahendra, and M. Surur, "Analisis Keamanan Jaringan Dari Serangan Malware Menggunakan Filtering Firewall Dengan Port Blocking," 2023. doi: 10.47709/digitech.v3i2.3379.
 - [10] S. Safiuddin and F. P. E. Putra, "Strategi Efisiensi Wireless Sensor Network (WSN)," *INFORMATICS Educ. ...*, 2023, [Online]. Available: <http://101.255.92.196/index.php/ITBI/article/view/2441>
 - [11] F. P. E. Putra, D. E. Arissandi, A. Rofiqi, and M. F. Hidayat, "Pemanfaatan Mikrotik Dalam Manajemen Bandwidth Pada Jaringan Sekolah," 2025, *researchgate.net*. [Online]. Available: https://www.researchgate.net/profile/Fauzan-Eka-Putra-2/publication/392420575_Pemanfaatan_Mikrotik_Dalam_Manajemen_Bandwidth_Pada_Jaringan_Sekolah/links/6848fab46b5a287c304a61ca/Pemanfaatan-Mikrotik-Dalam-Manajemen-Bandwidth-Pada-Jaringan-Sekolah.pdf
 - [12] L. Kaur and R. Kaur, "Fog-Based Energy Efficient Routing Protocol for Smart Building Evacuations," *Wirel. Pers. Commun.*, vol. 139, no. 1, pp. 543–571, 2024, doi: 10.1007/s11277-024-11637-8.
 - [13] U. Nath, S. Banerjee, C. Santini, R. Citroni, F. Mangini, and F. Frezza, "Simple and Cost-Effective Design of a THz-Metamaterial-Based Hybrid Sensor on a Single Substrate," *Sensors*, vol. 25, no. 12, 2025, doi: 10.3390/s25123660.
 - [14] J. Maeng, I. Park, J. Jeon, H. Kim, H. Lee, and C. Kim, "A Tri-Mode Reconfigurable DC-DC Converter With Photovoltaic Energy Harvesting for Miniature IoT Batteries," *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 71, no. 12, pp. 4844–4848, 2024, doi: 10.1109/TCSII.2024.3437449.
 - [15] M. Guri, "AIR-FI: Leaking Data From Air-Gapped Computers Using Wi-Fi Frequencies," *IEEE Trans. Dependable Secur. Comput.*, vol. 20, no. 3, pp. 2547–2564, 2023, doi: 10.1109/TDSC.2022.3186627.
 - [16] S. A. Murad and N. Rahimi, "Secure and Efficient Hierarchical P2P Fog Architecture: A Novel Approach for IoT," *IEEE Internet Things J.*, vol. 11, no. 10, pp. 18796–18807, 2024, doi: 10.1109/JIOT.2024.3365071.
 - [17] A. Wasay Mudasser and S. A. Ahmed Abdul Gafoor, "Secure Internet of Things based hybrid optimization techniques for optimal centroid routing protocol in wireless sensor network," *Concurr. Comput. Pract. Exp.*, vol. 35, no. 6, p. 1, 2023, doi: 10.1002/cpe.7585.
 - [18] N. T. Mahmoud, R. Shaltaf, M. Alyami, M. Alshaaer, and R. Habib, "Ab initio stability to efficiency study of SrGeO3 perovskite," *MRS Energy Sustain. - A Rev. J.*, vol. 11, no. 2, pp. 647–658, 2024, doi: 10.1557/s43581-024-00105-2.
 - [19] C. Okoh, W. N. Theophilus, P. Dawkins, and S. Paheerathan, "Enhancing Data Security Through VLSM Subnetting and TCP/IP Model in an ENT," *Appl. Sci.*, vol. 14, no. 23, 2024, doi: 10.3390/app142310968.
 - [20] J. Pennekamp *et al.*, "An Interdisciplinary Survey on Information Flows in Supply Chains," *ACM Comput. Surv.*, vol. 56, no. 2, 2024, doi: 10.1145/3606693.
 - [21] X. Qiu, S. Zhang, Z. Wang, and H. Luo, "Integrated Host- and Content-Centric Routing for Efficient and Scalable Networking of UAV Swarm," *IEEE Trans. Mob. Comput.*, vol. 23, no. 4, pp. 2927–2942, 2024, doi: 10.1109/TMC.2023.3267451.
 - [22] Z. Fang *et al.*, "Towards System-Level Security Analysis of IoT Using Attack Graphs," *IEEE Trans. Mob. Comput.*, vol. 23, no. 2, pp. 1142–1155, 2024, doi: 10.1109/TMC.2022.3231567.
 - [23] W. Sheng and H. Xiang, "A piezoelectric tuned mass damper for simultaneous vibration control and energy harvesting," *Smart Mater. Struct.*, vol. 33, no. 1, 2024, doi: 10.1088/1361-665X/ad1317.
 - [24] Z. Zhou *et al.*, "iMGC: Interactive Multiple Graph Clustering With Constrained Laplacian Rank," *IEEE Trans. Human-Machine Syst.*, vol. 53, no. 2, pp. 427–437, 2023, doi: 10.1109/THMS.2022.3227181.
 - [25] S. Liu *et al.*, "Harvesting energy from arbitrary horizontal vibration through a quad-stable magnetic rolling

- pendulum,” *Smart Mater. Struct.*, vol. 34, no. 7, 2025, doi: 10.1088/1361-665X/adea24.
- [26] M. B. Mandev, A. Altunkaynak, and A. Çelik, “Enhancing wave energy harvesting: Performance analysis of a dual chamber oscillating water column,” *Energy*, vol. 290, 2024, doi: 10.1016/j.energy.2023.130191.
- [27] N. Bermad, S. Zemmoudj, L. Bouallouche-Medjkoune, and L. Khoukhi, “Pseudonym revocation system for IoT-based medical applications,” *Comput. Networks*, vol. 257, 2025, doi: 10.1016/j.comnet.2024.110983.
- [28] D. R. D. Santos *et al.*, “Toward Indoor Simulations of OPV Cells for Visible Light Communication and Energy Harvesting,” *IEEE Access*, vol. 12, pp. 41027–41041, 2024, doi: 10.1109/ACCESS.2024.3378056.
- [29] T. Tao, L. Yan, W. Zhao, S. Liu, and H. Wang, “Low-Vibration Fault-Tolerant Control for Five-Phase PMSM Using Modified SVPWM and Random Modulation Strategy,” *IEEE Trans. Transp. Electr.*, vol. 11, no. 2, pp. 6775–6787, 2025, doi: 10.1109/TTE.2024.3516125.
- [30] I. S. Lacerda *et al.*, “Comparative Analysis of Piezoelectric Transducers for Low-Power Systems: A Focus on Vibration Energy Harvesting,” *Appl. Sci.*, vol. 14, no. 20, 2024, doi: 10.3390/app14209451.
- [31] B. V. Minh, T. N. Nguyen, and L.-T. Tu, “Physical layer security in wireless sensors networks: secrecy outage probability analysis,” *J. Inf. Telecommun.*, vol. 9, no. 1, pp. 1–23, 2025, doi: 10.1080/24751839.2024.2352961.
- [32] N. Panayanthatta *et al.*, “Electro-Mechanical Characterization and Modeling of a Broadband Piezoelectric Microgenerator Based on Lithium Niobate,” *Sensors*, vol. 24, no. 9, 2024, doi: 10.3390/s24092815.
- [33] S. Ali, M. Nadeem, S. Ahmed, M. A. Ullah, and M. Tahir, “3D Dynamic Topology With Energy-Aware Forwarding in Underwater Acoustic Networks (MAEARS),” *IEEE Access*, vol. 12, pp. 129319–129329, 2024, doi: 10.1109/ACCESS.2024.3434651.
- [34] M. Qaraqe *et al.*, “PublicVision: A Secure Smart Surveillance System for Crowd Behavior Recognition,” *IEEE Access*, vol. 12, pp. 26474–26491, 2024, doi: 10.1109/ACCESS.2024.3366693.
- [35] G. Uganya and R. M. Bommi, “New key added signature scheme for enhancement of security in IOT blockchain network,” *J. Supercomput.*, vol. 81, no. 15, 2025, doi: 10.1007/s11227-025-07914-3.
- [36] W. Villegas-Ch, J. Garcia-Ortiz, and S. Sanchez-Viteri, “Educational Advances in the Metaverse: Boosting Learning Through Virtual and Augmented Reality and Artificial Intelligence,” *IEEE Access*, vol. 12, pp. 59093–59112, 2024, doi: 10.1109/ACCESS.2024.3393776.
- [37] M. A. Saporin, H. Salleh, C. K. Hen, and S. N. A. Amnuruddin, “Performance of A Triboelectric Nanogenerator Utilising Coconut Husk Layer,” *J. Mech. Eng.*, vol. 21, no. 3, pp. 123–143, 2024, doi: 10.24191/jmeche.v21i3.27350.
- [38] Y. Chi, C. Lin, J. Deng, K. Ning, X. Fan, and G. Wu, “Edge Computing Underwater Optical Wireless Sensor Networks,” *IEEE Trans. Mob. Comput.*, vol. 24, no. 11, pp. 11879–11895, 2025, doi: 10.1109/TMC.2025.3581690.
- [39] S. B. Mallikarjun, M. Asif Habibi, M. Dixit, X. Costa-Pérez, M. Debbah, and H. D. Schotten, “Exploring Y1 Communications and Services in O-RAN: Background, Privacy, and Security,” *IEEE Open J. Commun. Soc.*, vol. 6, pp. 4638–4666, 2025, doi: 10.1109/OJCOMS.2025.3572709.
- [40] S. SeyedShenava, P. Zare, and I. F. Davoudkhani, “Maximizing solar energy harvesting efficiency: Optimal hybrid deep neural learning - based MPPT for Photovoltaic systems under complex partial shading conditions,” *Sustain. Comput. Informatics Syst.*, vol. 47, 2025, doi: 10.1016/j.suscom.2025.101159.
- [41] Y. Wang *et al.*, “Multifunctional bio-aerogels realized by solvophilic phase assisted phase separation for passive radiative cooling and energy harvesting,” *Chem. Eng. J.*, vol. 512, 2025, doi: 10.1016/j.cej.2025.162059.
- [42] N. Rodday *et al.*, “The Resource Public Key Infrastructure (RPKI): A Survey on Measurements and Future Prospects,” *IEEE Trans. Netw. Serv. Manag.*, vol. 21, no. 2, pp. 2353–2373, 2024, doi: 10.1109/TNSM.2023.3327455.
- [43] K. Psarftis, K. S. Ntalianis, and N. E. Mastorakis, “Quality of Experience Oriented Eco-Friendly Taxi-Ride Sharing Recommendation Framework,” *IEEE Access*, vol. 12, pp. 155915–155942, 2024, doi: 10.1109/ACCESS.2024.3485221.
- [44] W. Liu, “Pyas: Pay for Your Aggregation Service—A Privacy Preserving Aggregation Protocol of Time-series Data,” *Wirel. Pers. Commun.*, vol. 132, no. 1, pp. 757–773, 2023, doi: 10.1007/s11277-023-10637-4.
- [45] L. Zhang, Y. Du, and Z. Sun, “Modeling and Analysis of Cascading Failures in LEO Satellite Networks,” *IEEE Trans. Netw. Sci. Eng.*, vol. 11, no. 1, pp. 807–822, 2024, doi: 10.1109/TNSE.2023.3308610.
- [46] H. Alimohammadi, K. Vassiljeva, S. H. HosseinNia, and E. Petlenkov, “Bandgap Dynamics in Locally Resonant Metastructures: A General Theory of Internal Resonator Coupling,” *Appl. Sci.*, vol. 14, no. 6, 2024, doi: 10.3390/app14062447.
- [47] M. Sharmila and R. V. S. Satyanarayana, “An intelligent resource allocation strategy for machine type

- communication environment,” *Int. J. Commun. Syst.*, vol. 37, no. 1, 2024, doi: 10.1002/dac.5628.
- [48] A. Renaldo Maximus and S. Balaji, “Energy-Efficient Fuzzy Logic With Barnacle Mating Optimization-Based Clustering and Hybrid Optimized Cross-Layer Routing in Wireless Sensor Network,” *Int. J. Commun. Syst.*, vol. 38, no. 5, 2025, doi: 10.1002/dac.6132.
- [49] C. Wang, S. Chen, H. Hu, and X. Fan, “A distributed cluster-based routing protocol using fuzzy logic and deep reinforcement learning for wireless sensor networks,” *Cluster Comput.*, vol. 28, no. 8, 2025, doi: 10.1007/s10586-025-05206-2.
- [50] P. V. Bhosale and S. D. Agashe, “Investigation and hybrid deep belief neural network-based validation of piezoelectric bimorph cantilever composites assisted with tip mass,” *Noise Vib. Worldw.*, vol. 55, no. 1–2, pp. 3–15, 2024, doi: 10.1177/09574565231212688.
- [51] J. Goedhart, “Studentsourcing—Aggregating and reusing data from a practical cell biology course,” *PLOS Comput. Biol.*, vol. 20, no. 2, 2024, doi: 10.1371/journal.pcbi.1011836.
- [52] M. D. Hussain, B. Dudem, D. I. Kutsarov, and S. R. P. Silva, “Exploring charge regeneration effect in interdigitated array electrodes-based TENGs for a more than 100-fold enhanced power density,” *Nano Energy*, vol. 130, 2024, doi: 10.1016/j.nanoen.2024.110112.

Publisher’s Note: Publisher stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.