PT Mekar Research and Publishing
MIKIR : Mathematics, Informatics, Knowledge And Information Research
ISSN : 3110-7699 (Online)
Url : https://mikir.org/mikir

Contemporary Computer Network Infrastructure Transformation: Performance Management, Internet of Things (IoT) Convergence, and Cybersecurity Resilience

Muhammad Zaky Adima Putra[1]*, Ima Firda Fradilla[1], Fauzan Masykur[1]
[1]Program Studi Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Ponorogo
Jl Budi Utomo No 10, Ponorogo, Indonesia
*Corresponding Author Email: m.zakyadima.p@gmail.com

Doi : https://doi.org10.65475/1ekhdb44

Key-Words :
Network Architecture, Bandwidth Management, Mikrotik, Internet of Things, Cybersecurity, Vocational Education, 5G Network, Zero Trust.

Received : May 3, 2026.
Revised : May 10, 2026.
Published : May 29, 2026

Abstract

The development of information technology over the past decade has demanded a massive restructuring of computer network architecture. Infrastructure that previously focused solely on local area network (LAN) connectivity has now radically transformed into a hybrid ecosystem that integrates cloud computing, Software-Defined Networking (SDN) infrastructure, billions of 5G-enabled Internet of Things (IoT) devices, and demands a layered cybersecurity architecture powered by artificial intelligence (AI). This article aims to present a comprehensive literature review of three key pillars of modern computer networks: (1) performance optimization through automated bandwidth management and AI-driven QoS implementation; (2) network convergence and scalability to accommodate IoT devices in the agriculture, civil infrastructure, and logistics sectors; and (3) cybersecurity risk mitigation amidst an expanding attack surface. Using a systematic literature review, this study identifies that the implementation of intelligent traffic management not only reduces latency but also maintains stability (throughput). Furthermore, IoT integration requires 5G connectivity and lightweight communication protocols for high availability. This increased interconnectivity has serious implications for cyber resilience, urgently requiring the implementation of Zero Trust architecture, machine learning-based intrusion detection, and regular encryption system updates. This article provides a strong theoretical foundation for the development of future network infrastructure while highlighting the importance of preparing human resources through vocational education in information technology.

1. INTRODUCTION

Jaringan komputer sejatinya adalah tulang punggung dari peradaban digital yang kita rasakan saat ini. Kalau kita tilik secara definitif, jaringan komputer merupakan sekumpulan interkoneksi antar-perangkat otonom yang saling bertukar informasi dan berbagi sumber daya lewat berbagai media transmisi, mulai dari bentangan kabel serat optik bawah laut hingga transmisi gelombang nirkabel. Seiring dengan pergeseran dunia dari revolusi industri 4.0 menuju era *Society 5.0*, parameter untuk menilai kualitas sebuah jaringan tidak lagi sekadar melihat apakah statusnya "terhubung" atau tidak. Di era ini, jaringan dituntut untuk memenuhi standar ketat terkait latensi (*delay*), *throughput* (kapasitas data aktual), *high availability*, serta ketahanan (*resilience*) terhadap serangan intrusi dari pihak luar. Ancaman siber di era *Society 5.0* makin masif, sehingga inovasi dalam menjaga stabilitas sosial dan keamanan data telah menjadi prioritas pertahanan [1].

Dinamika arsitektur jaringan saat ini sangat kencang didorong oleh digitalisasi hampir di seluruh sektor kehidupan. Sektor pendidikan, pemerintahan, infrastruktur publik, hingga ritel daring (*e-commerce*) memiliki ketergantungan yang absolut terhadap infrastruktur pertukaran data. Kondisi operasional yang makin rumit ini pada akhirnya memaksa para *network administrator* atau insinyur jaringan untuk merancang topologi yang benar-benar bisa di-*scale-up* kapan saja. Menariknya, konsep dan sejarah evolusi teknologi *Internet of Things* (IoT) membuktikan bahwa lompatan dari miliaran perangkat pasif menjadi perangkat cerdas menuntut infrastruktur yang sama sekali berbeda dari era internet awal [2].

Ada beberapa ironi di balik kemajuan *hardware* seperti *switch gigabit* atau perangkat *router* berbasis prosesor *multi-core*. Tantangan terbesarnya justru sering mangkal di lapisan pengelolaannya (*management layer*). Alokasi *bandwidth* yang berantakan sering kali menjadi biang kerok inefisiensi dalam jaringan institusi. Belum lagi saat infrastruktur lokal ini harus disandingkan dengan sensor-sensor IoT yang tiada henti mengirimkan metrik data dalam ukuran kecil secara *real-time*. Kalau tidak ada

otomatisasi manajemen jaringan yang baik, lalu lintas data akan berbenturan dan mengakibatkan *bottleneck* parah [3]. Selain perkara *hardware* dan *routing protocol*, kita tidak bisa menutup mata terhadap aspek *human error* dan penyiapan Sumber Daya Manusia (SDM). Ekosistem digital butuh teknisi yang tidak cuma jago pasang kabel, tapi juga paham cara mitigasi risiko. Sekolah menengah kejuruan (SMK) dan pendidikan vokasi memainkan peran vital di sini. Pada akhirnya, perpaduan antara inovasi teknologi arsitektur jaringan, adaptasi IoT, pengamanan data lintas sektor, dan kesiapan talenta digital adalah sebuah roda ekosistem yang saling menggerakkan. Kajian literatur dalam artikel ini akan mengeksplorasi secara mendalam elemen-elemen tersebut berdasarkan temuan penelitian mutakhir.

2. METHODS

Penelitian ini menggunakan metode Tinjauan Literatur Sistematis (Systematic Literature Review atau SLR). Metode ini dipilih karena tujuan utama dari penelitian ini adalah untuk mengidentifikasi, mengevaluasi, dan menginterpretasikan seluruh temuan penelitian mutakhir yang relevan dengan fenomena transformasi infrastruktur jaringan komputer kontemporer. Melalui pendekatan SLR, kajian ini tidak hanya sekadar merangkum penelitian terdahulu, melainkan melakukan sintesis kritis terhadap pergeseran paradigma dari jaringan konvensional menuju ekosistem hibrida yang melibatkan komputasi awan, IoT, dan keamanan siber.

Proses pengumpulan data dilakukan secara sekunder dengan menelusuri literatur melalui berbagai basis data akademik, seperti Google Scholar, IEEE Xplore, dan portal jurnal nasional maupun internasional. Kata kunci yang digunakan dalam proses pencarian literatur meliputi "Arsitektur Jaringan", "Manajemen Bandwidth", "Software-Defined Networking", "Internet of Things", "Zero Trust Architecture", dan "Keamanan Siber". Untuk memastikan relevansi dan kebaruan informasi (state-of-the-art), literatur yang dipilih difokuskan pada artikel jurnal, prosiding konferensi, dan laporan akademik yang dipublikasikan dalam rentang waktu lima tahun terakhir (mayoritas literatur tahun 2023 hingga 2025), dengan memprioritaskan publikasi yang telah melalui proses peer-review.

Setelah literatur terkumpul dan diseleksi berdasarkan kriteria inklusi, tahap selanjutnya adalah analisis data menggunakan teknik sintesis tematik. Ribuan halaman data dari puluhan artikel tersebut dibedah dan dikelompokkan ke dalam beberapa domain pembahasan utama. Domain tersebut mencakup optimalisasi kinerja jaringan (QoS dan manajemen bandwidth), konvergensi infrastruktur IoT dan jaringan 5G di berbagai sektor publik, serta mitigasi ancaman keamanan siber di era jaringan terbuka. Melalui kategorisasi tematik ini, benang merah antara tantangan teknis jaringan, kesiapan sumber daya manusia (vokasi), dan solusi arsitektur keamanan siber dapat ditarik menjadi sebuah kesimpulan yang utuh.

3. RESULTS AND DISCUSSION

Arsitektur Jaringan Komputer Modern dan Manajemen *Bandwidth*

Sadar atau tidak konsep konvensional di mana kita membangun *Local Area Network* (LAN) yang kaku dan terisolasi kini telah usang. Industri sudah lama melangkah menuju arsitektur *Software-Defined Networking* (SDN) dan *Software-Defined Wide Area Network* (SD-WAN). Pada arsitektur jadul, seorang teknisi harus membuka konsol pada tiap-tiap *router* dan *switch* secara manual untuk mengonfigurasi rute jaringan. Ketika diterapkan pada jaringan skala korporat dengan ribuan *node*, pendekatan ini bukan cuma makan waktu, tapi juga rawan kesalahan konfigurasi.

Arsitektur SDN mengubah peta permainan dengan cara memisahkan fungsi lalu lintas paket (*data plane*) dari otak peruteannya (*control plane*). Lewat sebuah *centralized controller* berbasis perangkat lunak, administrator bisa memberikan instruksi penyesuaian rute dinamis ke ratusan *switch* sekaligus. Analisis pada infrastruktur SDN secara nyata membuktikan bahwa metode kontrol terpusat ini ampuh mereduksi *delay* pengiriman paket, menekan variasi keterlambatan (*jitter*), serta meningkatkan besaran *throughput* dibandingkan topologi konvensional [4]. Ini membuat otomatisasi pembuatan *Virtual Local Area Network* (VLAN) untuk memisahkan lalu lintas antar divisi kerja menjadi sangat mudah dan meminimalisir tabrakan *broadcast domain* yang membebani CPU keras [20].

Lebih jauh lagi, rancangan manajemen jaringan masa kini tak lagi dipisahkan dari otomatisasi pengelolaan perangkat keras dan komputasi awan. Dengan memadukan infrastruktur fisik dan perintah berbasis logika pemrograman, penyesuaian beban trafik bahkan bisa dilakukan tanpa ada intervensi manusia sama sekali saat terjadi *traffic spike* [3], [21].

Implementasi *Quality of Service* (QoS) dan Eksekusi Antrean

Masalah fundamental di setiap institusi adalah fakta bahwa tidak semua paket data derajatnya setara. Aplikasi rapat berbasis video, sistem *gaming* interaktif, atau transmisi data pemantauan jantung rumah sakit sangat rentan terhadap jeda waktu sepersekon detik. Sebaliknya, orang yang sedang mengunduh dokumen PDF tidak akan sadar kalau *file*-nya tertunda setengah detik. Solusi dari tumpang tindih ini adalah penerapan *Quality of Service* (QoS) di level *Network Layer*.

Untuk institusi skala kecil-menengah, eksekusi QoS masih banyak bergantung pada implementasi fitur antrean di perangkat Mikrotik. Praktik empiris menunjukkan bahwa ketiadaan batas pemakaian (limitasi) berisiko memicu monopoli *bandwidth* oleh segelintir alamat IP [5]. Dengan menerapkan algoritma *Simple Queue*, parameter batas kecepatan seperti *Maximum Information Rate* (MIR) dan *Committed Information Rate* (CIR) dapat dikunci secara logis. *Router* akan dengan cerdas membuang (*drop*) paket TCP/UDP dari IP klien yang rakus sehingga memaksa perangkat ujung (*endpoint*) untuk merendahkan *window size* transmisi secara otomatis. Teknik yang lebih

kompleks, seperti *Queue Tree* yang dipadukan dengan *Hierarchical Token Bucket* (HTB), sering diuji komparasinya untuk memastikan pembagian *bandwidth* sisa yang adil berdasarkan status prioritas akademik maupun divisi korporat [22], [23].

Namun, masa depan QoS kini melangkah ke ranah yang lebih pintar. Tren teranyar menunjukkan keterlibatan kecerdasan buatan dalam mengambil alih pembagian *bandwidth* secara prediktif. Sistem AI bisa membaca kebiasaan lalu lintas jaringan sebuah institusi dan mengalokasikan efisiensi performa sebelum kemacetan benar-benar terjadi, mengurangi keluhan *end-user* secara drastis [6].

Konvergensi Jaringan dengan Ekosistem *Internet of Things* (IoT) dan 5G

Karakteristik Trafik IoT dan Katalisator 5G

Jika dibandingkan dengan kebiasaan manusia berselancar di dunia maya, cara perangkat *Internet of Things* (IoT) "berkomunikasi" sangatlah jauh berbeda. Perangkat seperti sensor kualitas udara, termostat cerdas, hingga kamera pendeteksi suhu tidak butuh puluhan Megabit per detik. Mereka biasanya hanya mengirim segelintir *byte* atau *kilobyte* data. Akan tetapi, mereka melakukan "teriakan" data ini ribuan kali dalam satu jam tanpa henti. Jika tidak dikelola dengan protokol yang benar, hal ini bisa mengakibatkan *overhead* yang menyiksa memori pada *router*. Itulah mengapa sistem pemantauan daya listrik banyak membuang protokol HTTP konvensional dan beralih ke protokol pub-sub ringan seperti MQTT (*Message Queuing Telemetry Transport*) yang beban kerjanya jauh lebih manusiawi terhadap *server* [24], [25].

Evolusi IoT tidak bisa lepas dari evolusi jaringan seluler. Keberadaan jaringan 5G bukan sekadar *gimmick* operator telekomunikasi, melainkan fondasi mutlak bagi implementasi sensor jarak jauh berkecepatan tinggi. Dalam analisis kinerja terbarunya, kehadiran 5G terbukti secara radikal memangkas batasan latensi pada transmisi data antar mesin (M2M) sehingga memungkinkan respon IoT dalam hitungan milidetik [7]. Dengan dukungan kapasitas data yang sangat besar dan kecepatan tinggi dari 5G, isu otomatisasi peralatan cerdas menjadi makin mudah diimplementasikan, tanpa perlu mengorbankan stabilitas protokol pertukaran sistem kontrolnya [8].

Penerapan Lintas Sektor: Agrikultur, Infrastruktur, dan Smart City

Konvergensi jaringan ini mencetak dampak yang sangat merata. Di sektor agrikultur presisi, *routing* dan konektivitas tanpa kabel (seperti LoRaWAN atau *Narrowband* IoT) dihampar menembus lahan persawahan untuk memanen data metrik tanah [26]. Ketidakstabilan sinyal pada lahan terbuka memang menjadi momok, sehingga jika sistem tidak *reliable*, prediksi AI terkait jadwal panen dan pemupukan bakal meleset akibat banyaknya *packet loss* di perjalanan [27], [28]. Dengan protokol IoT berbasis *web*, petani modern bisa mengawasi konsumsi sumber daya perkebunannya layaknya mengawasi server data [29].

Beralih ke lanskap infrastruktur perkotaan dan *Smart City*, eskalasi penerapannya jauh lebih krusial. Penggunaan data analitik aktual dan sistem otomatisasi berbasis SCADA nyatanya terbukti vital dalam menjaga sistem distribusi daya listrik kota; mencegah fenomena mati lampu massal lewat pemantauan kondisi instrumen gardu listrik 24/7 [9]. Tidak hanya jaringan listrik, rancangan infrastruktur fasilitas sipil seperti keandalan jembatan dan bendungan juga mulai dijahit dengan teknologi pintar untuk deteksi dini kerusakan struktural [10]. Infrastruktur makro dari kampus percontohan yang memadukan manajemen tata kelola berbasis fiber optik menunjukkan bagaimana jaringan dinamis seperti *Open Shortest Path First* (OSPF) bisa menjaga konektivitas antar instrumen kampus dengan tingkat *uptime* nyaris sempurna meski ada kabel putus di satu titik [30], [31].

Ekonomi Digital, *Warehouse Management*, dan Penyiapan SDM

Akselerasi Layanan E-Commerce dan Pergudangan Cerdas

Ketahanan jaringan berbanding lurus dengan kelancaran ekonomi digital. Di industri *e-commerce*, keterlambatan server selama sepersekian detik bisa setara dengan hilangnya potensi pendapatan ratusan juta rupiah akibat *cart abandonment* oleh pelanggan. Analisis strategi perusahaan ritel menunjukkan tingginya urgensi infrastruktur komputasi untuk menyeimbangkan beban (*load balancing*) antarmuka web dan sinkronisasi stok toko luring ke aplikasi secara seketika [32]. Menariknya, sistem di luar toko pun tak luput dari intervensi digital. Transformasi digital dalam bentuk *Warehouse Management System* saat ini sangat bergantung pada jaringan IoT internal untuk otomasi alat pelacak barang inventaris, robot penarik kargo logistik, hingga sinkronisasi armada pengiriman [11]. Di tataran usaha mikro, stabilitas koneksi lewat teknologi jaringan *blockchain* dan internet turut diusulkan sebagai instrumen kemerataan ekonomi dan perlindungan transaksi di era *Society 5.0* [33]. Secara umum, ketahanan bisnis sebuah perusahaan di era modern ini tidak bisa dilepaskan dari keseriusan mereka menangani restrukturisasi digital dan ketahanan siber organisasinya [34].

Mencetak Tenaga Ahli Lewat Pendidikan Vokasional

Semua kecanggihan teknis ini tidak akan berumur panjang jika tidak ada teknisi "berdarah dingin" yang siap siaga memperbaikinya jika terjadi malfungsi jaringan fisik. Kurikulum SMK untuk program keahlian Teknik Komputer dan Jaringan dituntut bergerak agresif mengimbangi kebutuhan industri. Penggunaan media simulasi yang memancing kemampuan berpikir tingkat tinggi (HOTS) dikembangkan agar siswa bisa membayangkan wujud pergerakan lalu lintas data secara visual, bukan hanya menghafal teori buku [12]. Terobosan pendidikan kejuruan pun mulai diinkubasi di lingkungan pondok pesantren vokasi untuk mengakselerasi tingkat literasi teknologi pemuda di wilayah pinggiran agar memiliki daya tawar yang mumpuni dalam persaingan industri [13]. Namun, di saat bersamaan, ekosistem

jaringan sekolah itu sendiri rawan menjadi target peretasan, sehingga kurikulum pendidikan juga dituntut mendidik siswanya terkait etika dan teknik mengamankan *router* fasilitas belajar tempat mereka bernaung dari serangan IoT abal-abal [14].

Resiliensi Keamanan Siber di Tengah Infrastruktur Terbuka

Evolusi Serangan: Dari *DDoS*, *Man-in-the-Middle*, hingga Manipulasi IoT

Masifnya penambahan perangkat IoT dan adopsi komputasi awan menghancurkan garis batas (*perimeter*) jaringan tradisional korporat. Jika dahulu *firewall* sederhana cukup untuk menangkal penyusup dari luar, sekarang celah retas tersebar di setiap stopkontak pintar, kamera CCTV internet, dan titik *endpoint* lainnya. Kompleksitas tantangan keamanan siber di era IoT ini benar-benar membutuhkan peninjauan yang matang terkait protokol enkripsi apa yang sesuai, karena perangkat kecil biasanya tak mampu merender algoritma keamanan berat [15].

Jenis serangannya pun bermutasi. Fenomena *Distributed Denial of Service* (DDoS) kini kerap menggunakan botnet yang menginfeksi jutaan perangkat IoT rumahan untuk memberondong *server* sebuah institusi dengan *traffic* palsu [35]. Serangan lainnya seperti *Man-in-the-Middle* (MitM) sering menargetkan komunikasi jaringan berbasis kabel lokal dan jaringan nirkabel publik yang tidak menggunakan *tunneling* dengan benar [36]. Oleh karena itu, pengamanan *interface* pada mikrokontroler berbasis arsitektur *web service* menggunakan kunci penyandian berlapis seperti *Advanced Encryption Standard* (AES) adalah keharusan mutlak jika kita tidak ingin data sensor dimanipulasi orang tak bertanggung jawab [37]. Begitu pula implementasi rekapitulasi data krusial berskala nasional; investigasi terhadap insiden kebocoran *server* dan intrusi sistem publik semakin membuktikan bahwa kelemahan *port router* atau *SQL injection* bisa membawa malapetaka politik [38], [39]. Regulasi digital dan hukum kontrol akses di tataran negara mesti dirombak agar sejalan dengan keganasan era digital [40].

Strategi Mitigasi Terkini: AI, Deteksi Anomali, dan *Zero Trust Architecture*

Pendekatan keamanan lama terbukti tak lagi relevan untuk mempertahankan diri. Institusi modern saat ini bersandar pada model keamanan cerdas. Sebagai contoh, di ranah sistem kontrol industri atau *Industrial Control Systems* (ICS) yang rentan sabotase siber fisik, strategi perlindungan siber berbasis *Artificial Intelligence* (AI) mulai diterapkan untuk memeriksa anomali lalu lintas data perutean secara seketika [16]. Dalam konteks perkotaan, sistem AI spesifik menggunakan *Federated Learning* dikembangkan secara agresif untuk mendeteksi *cyberattacks* pada puluhan ribu sensor lalu lintas *Smart City* tanpa perlu memusatkan lalu lintas datanya ke satu tempat yang rawan diretas [41].

Bahkan di tingkatan arsitektur jaringan *Software-Defined Networking* (SDN), ancaman peretasan dapat dimitigasi menggunakan sistem deteksi dua arah yang cerdas; menggabungkan otentikasi visual (gambar) dengan detektor intrusi yang disokong model kecerdasan buatan, seperti kerangka *PictureGuard* [17]. Inovasi-inovasi berbasis sistem *machine learning* ini pada hakikatnya merupakan wujud nyata upaya menaikkan standar metrik "Cyber Resilience" atau ketahanan siber di ranah industri [18], [19].

Puncak dari evolusi sistem pengamanan logis ini bermuara pada implementasi *Zero Trust Architecture* (ZTA). Pada infrastruktur yang menerapkan konsep *Zero Trust*, tidak ada satupun entitas, alamat IP lokal, atau *device* atasan yang serta-merta dianggap "aman" oleh *router*. Meskipun kamu adalah CEO di kantor pusat, ketika laptopmu terhubung, kamu tetap diperlakukan seperti pendatang tak dikenal yang wajib melalui proses verifikasi berlapis, otorisasi sesi yang ketat, dan inspek paket secara mendalam (*Deep Packet Inspection*). Model arsitektur ini sudah diakui kemanjurannya dalam mengamankan arsitektur Industrial IoT (*IIoT*) yang tersebar di wilayah geografis berbeda [42]. Tanpa memadukan kedisiplinan VPN, *Intrusion Prevention System* (IPS), dan protokol SSH pada *router core*, konsep pelindung yang tangguh akan sekadar berujung pada mitos belaka.

4. CONCLUSION

Berpijak dari tinjauan yang telah dieksplorasi, dapat disimpulkan bahwa arsitektur jaringan komputer kontemporer telah menjelma menjadi sebuah organisme artifisial hibrida yang sangat kompleks. Ia tidak lagi terkurung dalam bentuk kotak *switch* di ruang server dingin, melainkan menjalar menyusuri fasilitas agrikultur pedesaan, menyokong pergerakan alat logistik *warehouse*, dan bertindak sebagai sistem syaraf pusat kelistrikan kota melalui teknologi sensor *Internet of Things* dengan dukungan gelombang mutakhir 5G. Pengelolaan sumber daya jaringan tak lagi bisa sekadar ditebak-tebak; pendekatan algoritma manajemen trafik pada skala mikro hingga otomatisasi komputasi awan yang diorkestrasi AI pada infrastruktur SDN menjadi prasyarat mutlak yang mendasari keandalan konektivitas tersebut.

Tetapi tingginya ketergantungan manusia pada "syaraf kabel dan gelombang radio" ini melahirkan ancaman keamanan dengan skala dan daya rusak yang jauh lebih mengerikan dibandingkan dekade sebelumnya. Serangan kini menggunakan pendekatan manipulatif pada tingkat lalu lintas yang menuntut hadirnya mekanisme deteksi intrusi berbasis *Machine Learning* dan pemberlakuan paradigma radikal seperti *Zero Trust Architecture* di setiap lini instansi. Di atas semua gemerlap perangkat keras canggih dan algoritma perutean dinamis tersebut, kedaulatan digital Indonesia pada akhirnya bersandar pada seberapa kompeten kita sanggup mengasah kemampuan anak muda bangsa melalui kurikulum pendidikan kejuruan yang peka terhadap mitigasi kerentanan sistem modern. Keselarasan antara optimasi fasilitas keras, pemantapan logika *resilience*, dan kualitas *brainware* inilah yang menjadi benteng pertahanan ekosistem data nasional di masa depan.

REFERENCES

[1] A. A. D. Aritonang, "Menghadapi ancaman siber di era society 5.0: Inovasi strategi diplomasi pertahanan untuk stabilitas sosial," *Jurnal Praksis dan Dedikasi Sosial*, 2025.

[2] A. Syahfitri, "Internet of Things (IoT), Sejarah, Teknologi, dan Penerapannya," *Uranus: Jurnal Ilmiah Teknik Elektro, Sains dan Informatika*, 2025.

[3] A. Firmansyah, M. F. Ramadhan, dan W. Wahyudi, "Rancangan Manajemen Jaringan dengan Integrasi Otomatisasi Menggunakan Internet of Things," *TAMIKA: Jurnal Tugas Akhir Manajemen Informatika & Komputerisasi Akuntansi*, 2024.

[4] H. P. Fitrian, A. Adkia, S. Rahmadani, R. P. Kencana, dan I. T. Fiddin, "Analisis Peningkatan Kinerja Jaringan Melalui Reduksi Delay, Jitter, dan Peningkatan Throughput pada Infrastruktur Software-Defined Networking di Digitech University," *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, 2025.

[5] A. Pratama dan B. Saputra, "Penerapan Metode Simple Queue untuk Manajemen Bandwidth dengan Router Mikrotik," *Practical Informatic and Technology Journal (PRACTIC)*, vol. 1, no. 1, hal. 30-37, 2025.

[6] U. J. Umoga dkk., "Exploring the potential of AI-driven optimization in enhancing network performance and efficiency," *Magna Scientia Advanced Research and Reviews*, 2024.

[7] F. Prasetyo dkk., "Analisis Kinerja Jaringan 5G dalam Meningkatkan Konektivitas Internet of Things (IoT)," *Jurnal Informatika Dan Tekonologi Komputer (JITEK)*, 2025.

[8] A. Yani, D. Irfansyah, S. Kurniawan, dan M. Muhidin, "Analisis Automation, Keamanan, dan Kecepatan Jaringan 5G dalam Implementasi Internet of Things (IoT)," *Journal of Mathematics and Technology (MATECH)*, 2024.

[9] M. Nuruzzaman dan S. Rana, "IOT-ENABLED CONDITION MONITORING IN POWER DISTRIBUTION SYSTEMS: A REVIEW OF SCADA-BASED AUTOMATION, REAL-TIME DATA ANALYTICS, AND CYBER-PHYSICAL SECURITY CHALLENGES," *Journal of Sustainable Development and Policy*, 2025.

[10] U. F. Arain, M. M. Afzal, dan A. S. Khokhar, "Integration of Smart Technologies and IoT in Civil Infrastructure Management," *Economic Sciences*, 2025.

[11] S. A. Gunawan, "Transformasi Digital dalam Warehouse Management: Eksplorasi Faktor Kunci Keberhasilan Implementasi Teknologi Internet of Things (IoT) pada Sistem Penyimpanan Barang," *Jupiter: Publikasi Ilmu Keteknikan Industri, Teknik Elektro dan Informatika*, 2025.

[12] P. P. S. Panggabean, "Pengembangan Media Pembelajaran Interaktif Berbasis Higher Order Thinking Skills (HOTS) pada Mata Pelajaran Dasar Teknik Jaringan Komputer dan Telekomunikasi di SMKN 14 Medan," Universitas Negeri Medan, 2024.

[13] G. D. Purwanto, "Inovasi Pendidikan Vokasi pada Sekolah Menengah Kejuruan Berbasis Pesantren di Kabupaten Cilacap," UIN Profesor Kiai Haji Saifuddin Zuhri, 2023.

[14] H. P. Fitrian, A. H. Munawar, B. N. Fajar, dan F. N. Aima, "Analisis Keamanan dan Ancaman pada Jaringan Komputer di Era Internet of Things (IoT) dalam Bidang Teknologi Sistem Pendidikan," *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, 2025.

[15] F. Kuswandi, A. Rukmana, dan A. Yanto, "KEAMANAN SIBER DALAM ERA INTERNET OF THINGS: TANTANGAN DAN SOLUSI TEKNOLOGI TERKINI," *Ipsikom*, 2025.

[16] J. H. Tarek dan W. Rahman, "AI-DRIVEN CYBERSECURITY, IOT NETWORKING, AND RESILIENCE STRATEGIES FOR INDUSTRIAL CONTROL SYSTEMS: A SYSTEMATIC REVIEW FOR U.S. CRITICAL INFRASTRUCTURE PROTECTION," *International Journal of Scientific Interdisciplinary Research*, 2023.

[17] H. S. Hatamleh dkk., "PictureGuard: Enhancing Software-Defined Networking–Internet of Things Security with Novel Image-Based Authentication and Artificial Intelligence-Powered Two-Stage Intrusion Detection," *Technologies*, 2025.

[18] M. Lezzi, A. Corallo, M. Lazoi, dan A. Nimis, "Measuring cyber resilience in industrial IoT: a systematic literature review," *Management Review Quarterly*, 2025.

[19] G.-Y. Yang, J.-N. Chen, F. Wang, dan K.-H. Yeh, "Enhancing Resilience for IoE: A Perspective of Networking-Level Safeguard," *IEEE Network*, vol. 40, hal. 59-68, 2025.

[20] D. Satria, "Penerapan VLAN pada VAP Menggunakan Mikrotik CAPsMAN untuk Manajemen Bandwidth Berbasis PCQ," vol. 5, no. 3, 2025.

[21] M. G. Seftian, M. Wildan, dan D. Pratama, "Perancangan Jaringan LAN dengan Server Cloud Storage: Studi Kasus Menggunakan Cisco Packet Tracer," *Jurnal Sistem Informasi*, vol. 3, no. 1, 2025.

[22] W. Darajat, D. Juardi, dan A. Solehudin, "MANAJEMEN BANDWIDTH MENGGUNAKAN HIERARCHICAL TOKEN BUCKET DENGAN PARAMETER QUALITY OF SERVICE PADA KAFE 99," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 7, no. 3, hal. 1688–1693, 2023.

[23] M. Fadhli dan K. Ardiansyah, "Analisis Perbandingan Metode Simple Queue Dan Queue Tree Untuk Optimalisasi Manajemen Bandwidth Pada Mikrotik SMKN 1 Al-Mubarkeya," *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, vol. 7, no. 1, hal. 80–88, 2024.

[24] N. G. Ardana, "Monitoring Penggunaan Daya Listrik menggunakan Protokol MQTT berbasis Web," t.t.

[25] I. Hidayatullah, M. H. Khairi, I. Maulana, dan F. P. E. Putra, "Analisis Protokol Keamanan Jaringan dalam Era Internet of Things (IoT)," *Infotek: Jurnal Informatika dan Teknologi*, 2025.

[26] F. Muhammad, A. Bhawiyuga, dan D. P. Kartikasari, "Analisis Kinerja Protokol LoRaWAN untuk Transmisi Data pada Skenario Urban Area," t.t.

[27] U. Khoirunnisa, "Implementasi IoT dalam Memprediksi Hasil Panen," Universitas Muhammadiyah Sumatera Utara, 2023.

[28] K. D. Irianto, "Evaluasi dan Analisis Kinerja LoRa Pada Sistem Irigasi Pertanian Berbasis IoT," *Open Science Framework*, 2022.

[29] A. M. Al Farizi dan M. Widyartono, "Monitoring Energi Listrik Generator Tenaga Surya Portabel Berbasis IoT Untuk Kebutuhan Listrik Didaerah Bencana," *JURNAL TEKNIK ELEKTRO*, vol. 12, no. 2, hal. 92–97, 2023.

[30] Universitas Indonesia, "Universitas Indonesia sebagai Model Kota Kampus Berkelanjutan dengan Teknologi Hijau untuk Energi Bersih Indonesia," Universitas Indonesia, 2024.

[31] E. S. Dirgantara, R. Primananda, dan W. Yahya, "Analisis Perbandingan Performa Protokol Routing OSPF, IGRP dan EIGRP pada Topologi Mesh dan Tree," t.t.

[32] R. Setiawan, "Analisis PESTEL dan Strategi Differensiasi dalam E-Commerce Erafone," *Digiventure: Journal of Business and Management*, vol. 2, no. 1, 2025.

[33] B. B. Sinaga dan R. P. N. Azzura, "Peran Teknologi Blockchain Sebagai Instrumen Pembangunan Penegakan Hukum Berbasis Digital & Mewujudkan Masyarakat Berkeadilan di Era Society 5.0," *Padjadjaran Law Review*, vol. 12, no. 1, 2024. [

34] S. Saeed, S. Altamimi, N. Alkayyal, E. Alshehri, dan D. Alabbad, "Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations," *Sensors*, vol. 23, 2023.

[35] A. S. Nasution dan W. Syafitri, "Analisis Serangan Man-In-The-Middle (Mitm) Dan Denial Of Service (Dos) Pada Protokol L2tp/Ipsec Berdasarkan Aspek Quality Of Service," vol. 4, 2025.

[36] M. A. Ajharie dan M. Sulistiyono, "IMPLEMENTASI FRAMEWORK MITM (MAN IN THE MIDDLE ATTACK) UNTUK MEMANTAU AKTIFITAS PENGGUNA DALAM SATU JARINGAN," *Jurnal Infomedia*, vol. 7, no. 1, hal. 45, 2022.

[37] A. Zubaidi dkk., "Pengamanan Internet of Things Berbasis NodeMCU Menggunakan Algoritma AES Pada Arsitektur Web Service REST," *Edumatic: Jurnal Pendidikan Informatika*, vol. 5, no. 2, hal. 252–260, 2021.

[38] A. P. Ashilah dan R. Rahman, "FORENSIK JARINGAN UNTUK INVESTIGASI KEJAHATAN CYBER PADA STUDI KASUS PEMBOBOLAN DATA KOMINFO OLEH BJORKA," vol. 1, no. 3, 2024.

[39] J. Thamrin, "Potensi Ancaman Cyber Crime di Pemilu Serentak 2024 di Indonesia," *Repository Universitas Bhayangkara Jakarta Raya*, 2023.

[40] M. Bahram, "REORIENTASI PERAN HUKUM DALAM MENGHADAPI DISRUPSI TEKNOLOGI: STUDI NORMATIF TENTANG REGULASI DIGITAL DI INDONESIA," *SINERGI : Jurnal Riset Ilmiah*, vol. 2, no. 3, hal. 1691–1702, 2025.

[41] I. Priyadarshini, "Anomaly Detection of IoT Cyberattacks in Smart Cities Using Federated

Learning and Split Learning," *Big Data and Cognitive Computing*, vol. 8, hal. 21, 2024.

[42] C. Zanasi, S. Russo, dan M. Colajanni, "Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures," *Ad Hoc Networks*, vol. 156, hal. 103414, 2024.