JUKOMTEK
(Jurnal Komputer Dan Teknologi)
e-ISSN 2961-9009
p-ISSN 2963-1289

ANALISIS TREN CYBERSECURITY PADA INFRASTRUKTUR JARINGAN KOMPUTER MODERN: SYSTEMATIC LITERATURE REVIEW

Ekoputra Wahyu Prakasa[1], Restu Nugianto[2], Yustian Servanda[3]

[1,2,3] Universitas Mulia, Kota Balikpapan Selatan, 76114
** Email Korespondensi: ekoputrawahyu28@gmail.com*

INFO ARTIKEL

Sejarah Artikel:
Diterima Tgl. 05/06/2026
Diperbaiki Tgl. 08/07/2026
Disetujui Tgl. 12/07/2026
Tersedia daring Tgl. 25/07/2026

e-ISSN 2961-9009
p-ISSN 2963-1289

DOI:
https://doi.org/10.64626/jukomtek.v5i2.685

Abstract: *The development of modern computer network infrastructure has become increasingly complex due to digital transformation, cloud computing, and interconnected devices, leading to significant growth in cybersecurity risks. This condition requires a comprehensive understanding of cybersecurity trends and challenges to strengthen network security systems. This study aims to identify and analyze the main trends and challenges in cybersecurity within modern computer network infrastructure. The research method used is a Systematic Literature Review with a systematic selection process, including identification, screening, and evaluation of relevant scientific articles published between 2021 and 2025. The results indicate that the main trends include the adoption of artificial intelligence for threat detection, the implementation of zero trust architecture, enhanced security in cloud environments, and the rise of automated cyber attacks. Meanwhile, the challenges involve increasing attack complexity, vulnerabilities in network devices, limited human resources in cybersecurity, and the expansion of the attack surface due to modern technology integration. In conclusion, adaptive, proactive, and intelligent technology-based security approaches are essential to address the evolving cybersecurity threats in modern computer network infrastructure.*

Keywords:
cybersecurity, computer networks, security trends, security challenges, systematic literature review

Abstrak: Perkembangan infrastruktur jaringan komputer modern yang semakin kompleks seiring digitalisasi, komputasi awan, dan perangkat terhubung menyebabkan peningkatan risiko keamanan siber yang signifikan. Kondisi ini menuntut pemahaman yang komprehensif terkait tren dan tantangan keamanan cybersecurity agar dapat mendukung penguatan sistem pertahanan jaringan. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis tren serta tantangan utama dalam keamanan cybersecurity pada infrastruktur jaringan komputer modern. Metode yang digunakan adalah Systematic Literature Review dengan pendekatan seleksi literatur secara sistematis melalui tahapan identifikasi, penyaringan, dan evaluasi terhadap artikel ilmiah yang relevan pada periode 2021 hingga 2025. Hasil penelitian menunjukkan bahwa tren utama meliputi pemanfaatan kecerdasan buatan dalam deteksi ancaman, penerapan arsitektur zero trust, peningkatan

E-ISSN : 2776-9666
P-ISSN : 2776-1789

keamanan pada lingkungan komputasi awan, serta berkembangnya serangan berbasis otomatisasi. Sementara itu, tantangan yang dihadapi mencakup meningkatnya kompleksitas serangan, kerentanan perangkat jaringan, keterbatasan sumber daya manusia di bidang keamanan, serta luasnya permukaan serangan akibat integrasi teknologi modern. Kesimpulan dari penelitian ini menunjukkan bahwa pendekatan keamanan yang adaptif, proaktif, dan berbasis teknologi cerdas sangat diperlukan untuk menghadapi dinamika ancaman cybersecurity pada infrastruktur jaringan komputer modern.

Kata Kunci:
cybersecurity, jaringan komputer, tren keamanan, tantangan keamanan, systematic literature review

PENDAHULUAN

Perkembangan pesat komputasi awan dan *internet of things* (IoT) telah memperluas konektivitas sekaligus meningkatkan risiko serangan pada jaringan komputer modern (Trend Micro 2025). Sebagai respons, sistem keamanan kini bertransformasi menjadi lebih proaktif melalui pemanfaatan kecerdasan buatan (AI) untuk mendeteksi ancaman dan penerapan *zero trust architecture* sebagai pengontrol akses (Netwrix, 2025).

Meskipun teknologi terus berkembang, kerentanan pada perangkat IoT, keterbatasan tenaga ahli, dan rendahnya kesadaran pengguna masih menjadi tantangan utama (Ade Irawan et al., 2024). Hal ini membuktikan bahwa efektivitas keamanan siber tidak hanya bergantung pada teknologi, tetapi juga pada sumber daya manusia (Muhamad Febrian Aska et al., 2025)

Menyikapi permasalahan tersebut, penelitian ini menggunakan metode *systematic literature review* terhadap publikasi ilmiah periode 2021 hingga 2025. Tujuannya adalah untuk mengidentifikasi tren ancaman dan menganalisis perkembangan teknologi keamanan terkini (Faizal et al., 2023), sehingga hasilnya dapat menjadi landasan yang kuat bagi pengembangan dan penelitian keamanan jaringan di masa depan.

LANDASAN TEORI

Cybersecurity

Cybersecurity (keamanan siber) adalah praktik yang digunakan untuk melindungi sistem komputer, jaringan, dan data-data penting dari ancaman atau serangan siber yang dapat menyebabkan kerusakan maupun gangguan pada sistem. Menurut penelitian terbaru,

E-ISSN : 2776-9666
P-ISSN : 2776-1789

perkembangan dunia komputer telah meningkatkan ancaman pada jaringan komputer modern (Al-Mhiqani et al., 2024).

Cybersecurity tidak hanya tentang perlindungan perangkat keras dan perangkat lunak, tetapi juga mencakup perlindungan bagi kerahasiaan dan ketersediaan informasi (Derri Anjuju et al., 2025). Dalam penerapannya, *cybersecurity* melibatkan berbagai macam teknologi keamanan, seperti *firewall*, sistem deteksi intrusi, hingga enkripsi data (Laksana & Mulyani, 2024). Selain itu, sumber daya manusia menjadi aspek penting dalam *cybersecurity*, karena pengguna harus memiliki kesadaran terhadap keamanan informasi dan bahaya serangan siber.

Infrastruktur Jaringan Komputer Modern

Infrastruktur jaringan modern, yang didukung oleh teknologi *cloud computing*, *internet of things* (IoT), dan virtualisasi jaringan, memang mempermudah pengelolaan data namun secara bersamaan meningkatkan risiko keamanan. Semakin banyaknya perangkat digital yang terhubung menyebabkan perluasan permukaan serangan (*attack surface*), yang menciptakan celah kerentanan baru (Gelgi et al., 2024). Khususnya, teknologi *cloud* dan perangkat IoT yang sering kali memiliki standar keamanan rendah, menjadi faktor utama yang rentan dieksploitasi untuk serangan siber seperti *denial of service* (DoS) (Zumhur Alamin & Muhammad Amirul Mu'min, 2025).

Tren Keamanan Cybersecurity

Perkembangan *cybersecurity* kini bertransformasi dari sistem reaktif menjadi proaktif dan adaptif (Safitri et al., 2025). Tren utama mencakup pemanfaatan kecerdasan buatan (*artificial intelligence*) untuk mendeteksi ancaman dan memberikan respons otomatis secara cepat dan akurat. Selain itu, keamanan modern menerapkan pendekatan *zero trust architecture* yang mewajibkan verifikasi ketat pada setiap upaya akses, tanpa memercayai entitas apa pun di dalam maupun di luar jaringan (Mushtaq et al., 2025). Fokus strategis lainnya adalah adopsi sistem keamanan berbasis *cloud* untuk pemantauan *real-time* guna memitigasi peningkatan ancaman otomatis seperti serangan *bot*.

Tantangan Keamanan Cybersecurity

Meskipun keamanan jaringan terus berkembang, penerapan *cybersecurity* masih menghadapi berbagai tantangan yang kompleks. Salah satunya adalah meningkatnya serangan siber yang memanfaatkan otomatisasi dan kecerdasan buatan untuk menemukan celah pada sistem secara lebih cepat dan tidak terdeteksi. Serangan modern saat ini tidak hanya menargetkan individu, tetapi juga perusahaan-perusahaan besar.

E-ISSN : 2776-9666
P-ISSN : 2776-1789

Tantangan lainnya adalah kerentanan pada perangkat *internet of things* yang sering kali tidak memiliki sistem keamanan yang memadai. Banyak perangkat terhubung yang jarang diperbarui, sehingga mudah dimanfaatkan oleh penyerang untuk melakukan pencurian data (Munawar et al., 2020).

Selain faktor teknologi, keterbatasan sumber daya manusia di bidang *cybersecurity* juga menjadi masalah krusial. Kurangnya tenaga ahli keamanan menyebabkan pengawasan terhadap sistem keamanan berjalan kurang optimal. Rendahnya kesadaran pengguna terhadap keamanan informasi juga meningkatkan risiko terjadinya serangan jaringan, seperti kebocoran data.

Systematic Literature Review

Systematic literature review (SLR) adalah metode evaluasi dan analisis berbagai penelitian terdahulu untuk memperoleh pemahaman mendalam mengenai suatu topik (Lutfina et al., 2024). Dalam penelitian ini, metode SLR diterapkan melalui tahapan terstruktur mulai dari pencarian, penyaringan, hingga penilaian kualitas jurnal untuk memetakan tren keamanan jaringan komputer modern. Tujuannya adalah untuk menghasilkan analisis yang komprehensif, objektif, dan relevan terkait perkembangan sistem keamanan berdasarkan literatur terbaru pada periode 2021 hingga 2025.

METODE PENELITIAN

Pendekatan Kajian Systematic Literature Review (SLR)

Penelitian ini menggunakan metode systematic literature review. Berbeda dengan tinjauan literature yang cenderung subjektif, SLR menerapkan kajian yang terstruktur agar mengurangi kesalahan seleksi melalui pencarian yang jelas, dan evaluasi kualitas yang kritis terhadap artikel yang dipilih sebagai acuan (Maelasari & Lusiana, 2025). seluruh tahapan dalam SLR dilakukan dengan standar internasional *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA).

Tabel 1. Kriteria Inklusi dan Eksklusi Pemilihan Literatur (SLR)

Parameter / KriteriaJurnal	Kriteria Inklusi (Inclusion Criteria)	Kriteria Eksklusi (Exclusion Criteria)
Rentang Waktu Publikasi	Artikel ilmiah yang diterbitkan dalam rentang tahun 2021 hingga 2025.	Artikel yang diterbitkan sebelum tahun 2021 atau setelah tahun 2025.
Jenis Dokumen	Artikel jurnal ilmiah (peer-reviewed journal) dan artikel prosiding konferensi ilmiah (conference proceedings) bereputasi.	Buku teks, bab buku (*book chapters*), artikel populer/opini, berita, laporan industri non-ilmiah, atau draf naskah

E-ISSN : 2776-9666
P-ISSN : 2776-1789

		yang tidak lengkap (*extended abstract*)..
Aksesibilitas Dokumen	Dokumen tersedia dalam bentuk teks lengkap (full-text available) dan dapat diunduh untuk dianalisis mendalam.	Dokumen yang hanya menyediakan abstrak, naskah terkunci (*paywall*), atau data teks lengkapnya rusak/tidak dapat diakses.
Bahasa	Artikel yang ditulis menggunakan Bahasa Indonesia atau Bahasa Inggris.	Artikel yang diterbitkan dalam bahasa selain Bahasa Indonesia dan Bahasa Inggris.
Substansi / Fokus Topik	Artikel yang membahas secara eksplisit mengenai tren teknologi keamanan dan tantangan siber pada infrastruktur jaringan modern (seperti Cloud Computing, Internet of Things (IoT), Zero Trust Architecture (ZTA), Software-Defined Security, dan implementasi AI/ML pada keamanan jaringan).	Artikel yang membahas keamanan siber pada perangkat *standalone* (PC tunggal), fokus pada kriptografi murni tanpa implementasi jaringan, atau bahasan *cybersecurity* makro yang tidak menyentuh arsitektur jaringan komputer kontemporer.
Kualitas & Validitas Metodologi	Artikel yang memiliki metodologi riset yang jelas, transparan, menyajikan data empiris, simulasi, atau sintesis konseptual yang valid untuk menjawab tren dan tantangan siber.	Artikel dengan metodologi yang tidak jelas/lemah, studi literatur konvensional yang tidak terstruktur, atau menyajikan redundansi teori dasar tanpa memberikan kontribusi temuan baru.

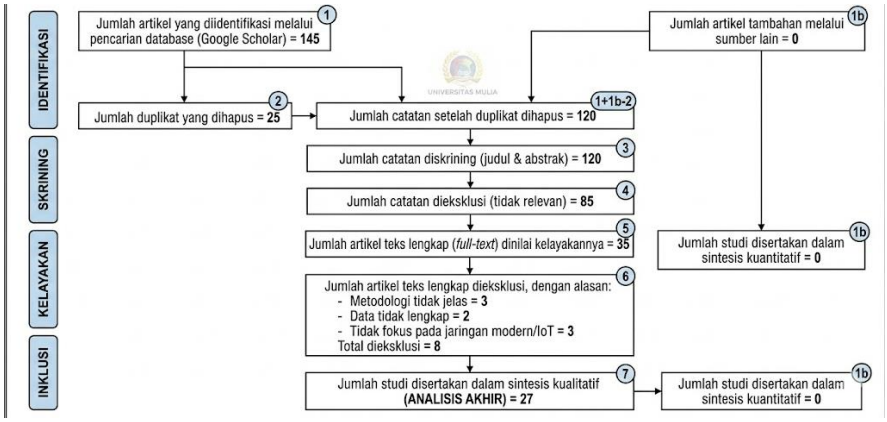
Untuk menerapkan kriteria inklusi dan eksklusi di atas terhadap dokumen yang ditemukan di basis data, dilakukan protokol penyaringan yang terbagi ke dalam beberapa tahapan seleksi secara bertahap. Hasil akumulasi dari pengurangan data tersebut dicatat secara sistematis pada Tabel 2.

Tabel 2. Protokol Seleksi Literatur Berdasarkan Alur Kerja PRISMA

Tahapan PRISMA	Prosedur Operasional & Modus Operandi	Jumlah Dokumen (n)	Keterangan / Alasan Eksklusi
Identifikasi	Pencarian entitas naskah pada database Google Scholar menggunakan kata kunci gabungan: ("cybersecurity" AND "computer networks" AND "security trends" OR "security challenges").	145	Batasan indeks publikasi global periode tahun 2021 hingga 2025.
Pra-Skrining	Pemeriksaan kesamaan identitas naskah, kesamaan metadata penulisan, dan sitasi ganda (overlapping datasets).	25	Dieliminasi secara otomatis dan manual karena duplikasi artikel.
Skrining	Peninjauan cepat terhadap relevansi naskah melalui pembacaan komparatif pada komponen Judul dan Abstrak.	120	Memasuki gerbang penyaringan kriteria inklusi operasional awal.

E-ISSN : 2776-9666
P-ISSN : 2776-1789

Eksklusi Awal	Pengeluaran naskah yang tidak memenuhi parameter substansi bahasan utama.	78	Dieksklusi karena: Fokus kajian berada di luar ekosistem jaringan modern (misal: hanya membahas PC *standalone*) atau tidak terbit pada korpus 2021–2025.
Kelayakan	Analisis konten secara menyeluruh (*full-text evaluation*) terhadap dokumen yang lolos skrining awal.	42	Pengujian integritas akademik terhadap draf artikel lengkap secara internal.
Eksklusi Akhir	Pengeluaran naskah hasil evaluasi mendalam draf lengkap (*full-text review evaluation*).	27	Dieksklusi karena: Metodologi SLR kurang transparan , analisis terlalu teoretis tanpa matriks empiris, atau terjadi duplikasi bahasan teoretis konvensional.
Diterima	Finalisasi jumlah artikel ilmiah yang dinyatakan valid dan relevan untuk dilakukan kodifikasi tematik.	15	Korpus Data Akhir: Terdistribusi penuh ke dalam 4 kluster taksonomi kualitatif utama pada bab hasil penelitian.



Gambar 1. Diagram Alur Seleksi Literatur Berdasarkan PRISMA

Systematic literature review (SLR) adalah metode terstruktur untuk mengidentifikasi dan mengevaluasi literatur guna meminimalkan bias subjektif dan menghasilkan temuan yang objektif. Dalam penelitian ini, metode SLR diterapkan melalui serangkaian tahapan—mulai dari pencarian, penyaringan, hingga seleksi artikel—untuk memetakan tren dan tantangan *cybersecurity* pada jaringan komputer modern. Berdasarkan literatur ilmiah periode 2021 hingga 2025, pendekatan ini diharapkan mampu memberikan gambaran dan analisis keamanan jaringan secara komprehensif.

Proses Ekstraksi dan Analisis Data

Tahap selanjutnya adalah ekstraksi data terstruktur dari 15 literatur terpilih ke dalam matriks analisis. Data dikategorikan berdasarkan penulis, tahun publikasi, fokus teknologi,

E-ISSN : 2776-9666
P-ISSN : 2776-1789

jenis ancaman, teori perilaku, dan efektivitas solusi yang diusulkan. Proses ini memadukan sintesis naratif kualitatif dan analisis deskriptif kuantitatif untuk memetakan sebaran studi dan risiko siber, guna menghasilkan kesimpulan riset yang kuat dan valid.

HASIL DAN PEMBAHASAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode *Systematic Literature Review* (SLR) untuk menganalisis tren *cybersecurity* pada jaringan komputer modern. Melalui *content analysis* dan reduksi data terhadap 15 artikel ilmiah terpilih, bab ini memaparkan karakteristik literatur, evolusi ancaman dan strategi pertahanan, serta efektivitas teknologi baru dalam mengatasi risiko siber saat ini.

Analisis Karakteristik Korpus Data dan Kodifikasi Tematik

Proses pemilihan literatur ini dilakukan berdasarkan panduan kerangka kerja PRISMA agar hasilnya valid dan dapat dipertanggungjawabkan secara akademis. Isu-isu utama dari 15 artikel ilmiah tersebut kemudian disederhanakan dan diklasifikasikan ke dalam kategori kualitatif yang lebih terstruktur. Pengelompokan ini bertujuan untuk memetakan fokus penelitian, sekaligus memudahkan penarikan kesimpulan terkait evolusi jaringan komputer modern saat ini.

Tabel 3. Taksonomi Kualitatif dan Distribusi Tematik Korpus Literatur

No	Kluster Tematis Jurnal	Jumlah Artikel	Fokus Eksplorasi Teoretis
1	Metodologi SLR, Tata Kelola, dan Kerangka Risiko Siber	5	Standardisasi tinjauan siber, taksonomi kerentanan, dan mitigasi risiko tata kelola organisasi.
2	Evolusi Vektor Serangan & Tren Ancaman	4	Komersialisasi Ransomware (RaaS), kerentanan inheren ekosistem IoT, dan pola operasional APT.
3	Teknologi Defensif dan Inovasi Cybersecurity	4	Optimasi Deep Learning untuk deteksi anomali dan DDoS, desentralisasi kontroler SDN via Blockchain, serta pertahanan siber aktif (active defense).
4	Dimensi Sosio-Ekonomi & Faktor Manusia	2	Kalkulasi kerugian finansial makro, rekayasa sosial (social engineering, dan pembentukan kesadaran siber.

E-ISSN : 2776-9666
P-ISSN : 2776-1789

Berdasarkan distribusi data di atas, kluster metodologi, tata kelola, dan kerangka risiko siber mendominasi dengan 5 artikel (33,3%), diikuti oleh kluster evolusi vektor serangan dan kluster teknologi defensif yang masing-masing berjumlah 4 artikel (26,7%), serta kluster dimensi sosio-ekonomi dan faktor manusia sebanyak 2 artikel (13,3%). Distribusi ini menunjukkan bahwa tren riset keamanan siber saat ini menekankan pemahaman terhadap standardisasi dan kompleksitas ancaman terlebih dahulu, sebelum merumuskan teknologi pertahanan yang lebih spesifik

Eksplorasi Teoretis Mutasi Lanskap Ancaman Kontemporer

Berdasarkan rangkuman literatur, adopsi teknologi seperti *hybrid cloud*, *edge computing*, dan *internet of things* (IoT) telah menyamarkan batas jaringan konvensional dan memperluas permukaan serangan (*attack surface*) (Al-Mhiqani et al., 2024; Nankya et al., 2023). Akibatnya, pola ancaman siber menjadi lebih kompleks. Serangan kini tidak hanya mengeksploitasi celah teknis tunggal, tetapi memanfaatkan interkoneksi antarlayanan untuk menargetkan berbagai komponen infrastruktur secara serentak (Shandilya et al., 2014).

Salah satu ancaman utama yang disorot adalah *Ransomware-as-a-Service* (RaaS). Model ini membuat kejahatan siber lebih terorganisasi dan terkomersialisasi (Fortinet, 2025), serta memicu kerugian finansial maupun operasional yang signifikan pada sektor kritis seperti perbankan (Analisis Risiko dan Keamanan dalam Layanan Perbankan Digital, 2024). Mayoritas serangan *ransomware* kini juga menggunakan taktik *double extortion*, yakni mengunci data sekaligus mengancam akan membocorkannya ke publik demi menekan korban (Fortinet, 2025).

Selain *ransomware*, kerentanan perangkat IoT juga menjadi fokus utama. Keterbatasan kapasitas komputasi pada IoT menyulitkan implementasi keamanan yang memadai (Al-Mhiqani et al., 2024). Hal ini membuat perangkat tersebut rentan menjadi pintu masuk serangan, terutama pada sektor infrastruktur kritis seperti rumah sakit pintar (*smart hospital*) dan sistem industri akibat lemahnya autentikasi (Gosálvez-White et al., 2025; Nankya et al., 2023).

Secara keseluruhan, transformasi infrastruktur jaringan modern telah mengubah karakteristik ancaman siber yang kini menargetkan seluruh ekosistem digital. Oleh karena itu, strategi pertahanan yang diterapkan mutlak harus beradaptasi untuk mengimbangi kompleksitas ancaman tersebut.

Dekonstruksi Paradigma Pertahanan: Zero Trust dan Software-Defined Security

E-ISSN : 2776-9666
P-ISSN : 2776-1789

Untuk mengimbangi perkembangan ancaman saat ini, banyak literatur keamanan siber mencatat adanya perubahan signifikan dalam prinsip perancangan keamanan jaringan. Model perlindungan konvensional yang menerapkan pendekatan *castle and moat* (istana dan parit) yang secara otomatis mengasumsikan aman setiap pengguna di dalam jaringan internal kini mulai ditinggalkan dan digantikan dengan model pertahanan yang lebih modern.

Prinsip Teoretis Zero Trust Architecture (ZTA)

Berdasarkan kajian literatur, *Zero Trust Architecture* (ZTA) kini menjadi tren utama untuk menggantikan keamanan perimeter konvensional yang tidak lagi memadai akibat masifnya adopsi *cloud*, perangkat *mobile*, dan *remote work* (Nahar et al., 2024). Mengusung prinsip "*never trust, always verify*", ZTA mewajibkan verifikasi akses berkelanjutan tanpa memercayai entitas mana pun, menjadikannya sangat relevan untuk infrastruktur masa depan seperti jaringan 5G dan 6G (Nahar et al., 2024).

Salah satu komponen kunci ZTA adalah *micro-segmentation*, yakni pembagian jaringan menjadi zona-zona kecil untuk membatasi ruang gerak peretas dan mencegah *lateral movement* jika terjadi intrusi (Shandilya et al., 2014). Selain memperkuat perlindungan jaringan, penerapan ZTA juga mengoptimalkan tata kelola informasi melalui pemantauan dan pencatatan akses yang terstruktur, sehingga menjadikannya fondasi esensial dalam strategi keamanan modern.

Orkestrasi Software-Defined Security (SDS) dan Keamanan SASE

Dengan adanya *Software-Defined Networking* (SDN), fungsi kontrol keamanan saat ini telah sepenuhnya dipindahkan dari perangkat keras fisik ke dalam lapisan perangkat lunak (*Software-Defined Security* atau SDS). Hasil analisis menunjukkan bahwa SDS membuat organisasi tidak lagi bergantung pada perangkat *firewall* fisik, karena sistem ini memungkinkan otomatisasi dan pengaturan kebijakan keamanan secara terpusat dan *real-time* di seluruh infrastruktur yang tersebar. Lebih lanjut, jika dikombinasikan dengan kerangka kerja *Secure Access Service Edge* (SASE), layanan keamanan jaringan dapat disatukan langsung melalui platform *cloud*. Hal ini tentu memberikan perlindungan yang konsisten bagi pekerja jarak jauh tanpa harus mengorbankan performa pengiriman data.

Analisis Integratif Teknologi Eksperimental (AI, Blockchain, dan Pertahanan Aktif)

Berdasarkan hasil kajian literatur, terlihat bahwa perkembangan *cybersecurity* modern saat ini tidak hanya berfokus pada peningkatan sistem pertahanan konvensional, tetapi juga melibatkan integrasi berbagai teknologi canggih yang dirancang untuk menghadapi ancaman yang semakin kompleks. Beberapa teknologi yang paling banyak

E-ISSN : 2776-9666
P-ISSN : 2776-1789

dibahas dalam penelitian periode tahun 2021 hingga 2025 di antaranya meliputi kecerdasan buatan (AI), *blockchain*, dan pertahanan siber aktif berbasis otomasi (active defense).

Artificial Intelligence (AI) dan Machine Learning (ML)

Penggunaan *Artificial Intelligence* (AI) dan *Machine Learning* (ML) kini mendominasi pengembangan sistem keamanan jaringan modern. AI mampu mengenali pola ancaman kompleks yang sulit dijangkau oleh metode konvensional (Kumar et al., 2021), sementara algoritma ML terbukti lebih adaptif dalam mengidentifikasi *malware* dan anomali jaringan dibandingkan metode *signature-based detection* (Kumar et al., 2021)

Selain itu, penerapan *Deep Learning* seperti *Convolutional Neural Networks* (CNN) efektif memproses data jaringan bervolume besar secara *real-time* untuk mendeteksi serangan DDoS (Batchu et al., 2024). Secara keseluruhan, peran AI saat ini telah berkembang dari sekadar alat deteksi menjadi sistem andalan untuk merespons insiden keamanan secara otomatis.

Blockchain untuk Otentikasi Terdesentralisasi

Jaringan modern menuntut mekanisme autentikasi yang aman dan kebal manipulasi. Teknologi *blockchain* menjawab kebutuhan ini melalui pendekatan terdesentralisasi yang meminimalkan ketergantungan pada pusat kendali tunggal (Guo dkk., 2023). Selain itu, penggunaan *smart contract* memungkinkan proses verifikasi identitas berjalan secara otomatis, transparan, dan autentik.

Sifat *blockchain* yang tidak dapat diubah (*immutable*) juga menjamin integritas catatan audit serta mencegah modifikasi data tanpa izin. Oleh karena itu, teknologi ini memiliki potensi besar dalam mendukung sistem keamanan pada infrastruktur jaringan masa depan, termasuk *Software-Defined Network* (SDN).

Pertahanan Siber Aktif dan Otomasi Countermeasure

Selain memperkuat lapisan pertahanan pasif, literatur terkini menyoroti pergeseran menuju pertahanan siber aktif (active cyber defense), yakni kemampuan sistem untuk mendeteksi, menipu, dan menetralkan penyerang secara otomatis sebelum kerusakan terjadi. Pendekatan berbasis deception dan pembelajaran otonom memungkinkan agen pertahanan mempelajari taktik lawan dan memilih countermeasure yang optimal secara mandiri pada lingkungan jaringan yang tersimulasi (Walter et al., 2021).

Untuk mendukung otomasi tersebut, pemodelan attack graph berperan penting dalam memetakan kombinasi kerentanan dan jalur serangan multi-tahap (multi-stage), sehingga administrator dapat memprioritaskan titik pertahanan yang paling kritis sekaligus merancang

E-ISSN : 2776-9666
P-ISSN : 2776-1789

respons yang efisien (Shandilya et al., 2014). Berdasarkan literatur, sinergi antara pertahanan aktif dan analisis jalur serangan dinilai menjanjikan untuk memperkuat ketahanan infrastruktur jaringan masa depan terhadap serangan yang semakin adaptif.

Matriks Komparasi dan Sintesis Kualitatif Terstruktur

Sebagai bentuk visualisasi data kualitatif dalam *Systematic Literature Review* ini, disusunsebuah tabel perbandingan (komparasi) yang terstruktur. Tabel ini memetakan fokus konsep, teknologi pertahanan yang diterapkan, target infrastruktur, hingga kesenjangan penelitian (*research gaps*) yang berhasil diidentifikasi dari kumpulan literatur tersebut.

Tabel 4. Matriks Sintesis Komparatif Hasil Literature Review

Kluster Korpus & Referensi	Fokus Konseptual	Model Defensif Utama	Target Infrastruktur	Tantangan dan Keterbatasan
Kluster SLR Keamanan	Standardisasi taksonomi ancaman global dan kodifikasi risiko siber.	Kerangka Manajemen Risiko Siber dan Tata Kelola Keamanan Informasi.	Enterprise Networks, Sektor Finansial.	Terlalu teoretis; kurang memberikan matriks pengukuran empiris instan untuk organisasi kecil
Tren Ancaman Makro	Analisis evolusi taktik pemerasan ganda malware dan ekosistem RaaS.	Threat Intelligence, IDS Berbasis AI, dan Cyber Threat Monitoring.	Hybrid Cloud, Data Center Terdistribusi.	Tingginya angka alarm palsu (false positives) pada pemantauan trafik terenkripsi.
Keamanan Ekosistem IoT	Eksplorasi kecacatan arsitektur IoT dan mitigasi serangan DDoS botnet.	Lightweight Cryptography, Network Access Control (NAC).	Edge Computing, Smart Hospital, IoT Industri.	Kompleksitas standardisasi akibat fragmentasi vendor perangkat keras yang ekstrem.
Arsitektur Telekomunikasi	Pengamanan komunikasi borderless pada core network seluler generasi maju.	Zero Trust Architecture (ZTA), Mikrosegmentasi Dinamis.	Jaringan Seluler 5G / 6G Core.	Timbulnya penumpukan latensi jaringan akibat verifikasi akses yang repetitif.
AI & Otomatisasi Cerdas	Deteksi proaktif anomali trafik jaringan tanpa signature manual.	Deep Learning, CNN, Behavioral Analysis.	Software-Defined WAN (SD-WAN).	Ketergantungan absolut pada kebersihan dataset latihan dan kerentanan terhadap serangan adversarial.
Desentralisasi & Enkripsi	Proteksi lapisan kendali (control plane) dari infiltrasi dan otomasi countermeasure adaptif.	Decentralized Blockchain, Smart Contract, Active Defense (deception).	SDN Controllers, Jaringan Enterprise Terdistribusi.	Masalah skalabilitas throughput konsensus rantai blok dan kompleksitas

E-ISSN : 2776-9666
P-ISSN : 2776-1789

pelatihan agen pertahanan otonom.

Diskusi Kritis, Paradoks Operasional, dan Agenda Riset Masa Depan

Implementasi teknologi keamanan modern menghadapi tantangan paradoksal, yakni peningkatan keamanan sering kali meningkatkan kompleksitas operasional sistem. Penerapan *Zero Trust Architecture* (ZTA), misalnya, menuntut autentikasi ketat yang menambah beban komputasi. Pada lingkungan *real-time* seperti jaringan 5G, otomasi industri, dan kesehatan digital, hal ini berisiko mengganggu performa layanan jika tidak dikelola dengan tepat (Nahar et al., 2024).

Di sisi lain, AI memiliki keterbatasan karena rentan terhadap *adversarial attacks* dan *data poisoning* (Batchu et al., 2024; Kumar et al., 2021). Oleh karena itu, AI sebaiknya diposisikan sebagai alat pendukung yang memerlukan pembaruan berkelanjutan, bukan solusi tunggal. Selain faktor teknologi, tantangan sumber daya manusia tetap krusial. Kurangnya kesadaran keamanan berkontribusi signifikan terhadap insiden siber (Evans et al., 2019), sementara *social engineering* masih menjadi metode peretasan yang efektif (Evans et al., 2019).

Kesimpulannya, masa depan *cybersecurity* bergantung pada integrasi multidimensi yang menyinergikan teknologi, tata kelola, kebijakan, dan budaya keamanan, bukan sekadar mengandalkan kecanggihan perangkat pertahanan.

KESIMPULAN DAN SARAN

Berdasarkan hasil *Systematic Literature Review* terhadap 15 artikel, konvergensi *cloud computing*, *edge computing*, dan IoT telah menghilangkan batas fisik jaringan dan memperluas permukaan serangan (*attack surface*). Hal ini memicu evolusi ancaman yang semakin kompleks, seperti *Ransomware-as-a-Service* (RaaS) dan *botnet*. Sebagai respons, strategi pertahanan kini beralih ke model adaptif berbasis identitas, yakni *Zero Trust Architecture* (ZTA) dengan prinsip "*never trust, always verify*" dan *micro-segmentation*. Pendekatan ini didukung oleh *Software-Defined Security* (SDS), kerangka SASE, *Deep Learning* untuk deteksi serangan *zero-day*, *blockchain* untuk manajemen akses terdesentralisasi, serta pertahanan siber aktif (active defense) berbasis otomasi. Namun, kecanggihan ini menghadirkan tantangan baru berupa peningkatan latensi akibat beban komputasi tambahan dan kerentanan AI terhadap *adversarial attacks*. Pada akhirnya, faktor manusia tetap menjadi titik terlemah dalam ekosistem keamanan siber.

E-ISSN : 2776-9666
P-ISSN : 2776-1789

Berdasarkan kesimpulan tersebut, rekomendasi praktis bagi industri adalah mengintegrasikan ZTA dengan akselerasi perangkat keras atau *network slicing* guna menekan latensi verifikasi akses tanpa mengorbankan keamanan. Selain itu, penguatan aspek manusia mutlak diprioritaskan melalui simulasi *phishing* dan pengetatan SOP untuk mitigasi ancaman *social engineering*. Dari sisi akademis, penelitian selanjutnya perlu merumuskan panduan arsitektur keamanan yang ringan dan aplikatif bagi sektor UMKM. Riset masa depan juga harus mengeksplorasi penguatan model AI melalui *adversarial training* terhadap *malware* polimorfik, optimasi *blockchain* berkecepatan tinggi, serta standardisasi kriptografi ringan yang efisien untuk perangkat IoT lintas vendor.

DAFTAR PUSTAKA

Ade Irawan, Wildan Hamzah Nur Fadholi, Zahwa Erikamaretha, & Fried Sinlae. (2024). Tantangan dan Strategi Manajemen Keamanan Siber di Indonesia berbasis IoT. *Journal Zetroem*, *6*(1), 114–119. https://doi.org/10.36526/ztr.v6i1.3376

Al-Mhiqani, M. N., Alsboui, T., Al-Shehari, T., Abdulkareem, K. hameed, Ahmad, R., & Mohammed, M. A. (2024). Insider threat detection in cyber-physical systems: a systematic literature review. *Computers and Electrical Engineering*, *119*(PA), 109489. https://doi.org/10.1016/j.compeleceng.2024.109489

Derri Anjuju, Suryayusra, S., Maria Ulfa, & Dedi Irawan. (2025). Analisis Keamanan Infrastruktur Teknologi Informasi Dalam Menghadapi Ancaman Cybersecurity. *Journal of Data Analytics, Information, and Computer Science*, *2*(1), 75–80. https://doi.org/10.70248/jdaics.v2i1.1792

Faizal, M. A., Faizatul, Z., Asiyah, B. N., & Subagyo, R. (2023). *ANALISIS RISIKO TEKNOLOGI INFORMASI PADA BANK SYARIAH : IDENTIFIKASI ANCAMAN DAN TANTANGAN TERKINI*. *5*(2), 87–100.

Gelgi, M., Guan, Y., Arunachala, S., Samba Siva Rao, M., & Dragoni, N. (2024). Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques. *Sensors*, *24*(11). https://doi.org/10.3390/s24113571

Laksana, T. G., & Mulyani, S. (2024). *PENGETAHUAN DASAR IDENTIFIKASI DINI DETEKSI SERANGAN KEJAHATAN SIBER UNTUK MENCEGAH PEMBOBOLAN DATA PERUSAHAAN*. *3*(1), 109–122.

Lutfina, E., Andriana, W., Wiratmaja, S. Q. P., & Febrianti, E. (2024). Metode dan Algoritma Dalam Sentimen Analisis: Systematic Literature Review. *Science Technology and Management Journal*, *4*(2), 67–79.

E-ISSN : 2776-9666
P-ISSN : 2776-1789

https://doi.org/10.53416/stmj.v4i2.274

Maelasari, N., & Lusiana. (2025). View of EFEKTIVITAS DEEP LEARNING DALAM PEMBELAJARAN: SEBUAH KAJIAN SYSTEMATIC LITERATURE REVIEW (SLR). *Education and Development*, *13*(2), 298–305. https://journal.ipts.ac.id/index.php/ED/article/view/7006/3712

Muhamad Febrian Aska, Deo Pratama Putra, & Sinambela, C. J. M. (2025). Strategi Efektif Untuk Implementasi Keamanan Siber di Era Digital. *Journal of Informatic and Information Security*, *5*(2), 187–200. https://doi.org/10.31599/fzg80847

Munawar, Z., Kom, M., & Putri, N. I. (2020). Keamanan Jaringan Komputer Pada Era Big Data. *Jurnal Sistem Informasi-J-SIKA*, *02*, 14–20.

Mushtaq, S., Mohsin, M., & Mushtaq, M. M. (2025). A Systematic Literature Review on the Implementation and Challenges of Zero Trust Architecture Across Domains. *Sensors*, *25*(19), 1–25. https://doi.org/10.3390/s25196118

Netwrix. (2025). *2025 cybersecurity trends report. Netwrix.* https://www.netwrix.com/2025-hybrid-security-trends-report.html

Safitri, U., Fauzi, A., Putri, D. A., Hutagalung, C. A., & Nursal, M. F. (2025). *Strategi yang Inovatif dan Progresif Dalam Budaya Sekuriti Menuju Masa Depan*. *2*(1), 23–32. https://doi.org/10.63217/fibonacci.v2i1.255

Zumhur Alamin, & Muhammad Amirul Mu'min. (2025). Analisis Keamanan Jaringan pada Sistem Kendali Jarak Jauh untuk Infrastruktur Kritis. *Jurnal Pengembangan Sains Dan Teknologi*, *1*(1), 25–41. https://doi.org/10.63866/jpst.v1i1.39