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

Computer Network Security: Challenges, Threats, and Protection Strategies in the Digital Era

Rayyan Faris Muhammad[1],'Ilma Nafi'atu Qorien[1], Ling Bachtiar A[1]
[1]Teknik Informatika, Universitas Muhammadiyah Ponorogo
Jl Budi Utomo No 10 Ponorogo, Indonesia
*Corresponding Author Email: rayyanhebat@gmail.com

Doi : https://doi.org/10.65475/e5fkj267

Key-Words :
network security, firewall, IDS/IPS, penetration testing, cyber threats

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

Abstract

Over the past few decades, rapid advances in information technology have brought about significant changes in the way people interact, communicate, and manage data. Conversely, these advancements have been accompanied by an increase in threats to computer network security. In this article, we will explore various aspects of computer network security, ranging from the most common types of threats, available protection technologies, to methods for successfully implementing security systems. This study collects, analyzes, and synthesizes various relevant scientific sources from Indonesian national journals published over the past five years (2021–2025). The findings indicate that cyber threats such as DDoS attacks, malware, brute force attacks, and SQL injection are increasingly prevalent, necessitating a layered approach to building network security systems. In the contemporary network security ecosystem, firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), Virtual Private Networks (VPN), data encryption, and penetration testing are essential. The conclusion of this article is that network security is not a product, but a process that must be updated and adapted in line with the evolution of cyber threats.

1. INTRODUCTION

Infrastruktur digital di berbagai bidang kehidupan, seperti bisnis, pemerintahan, pendidikan, dan layanan kesehatan, sangat bergantung pada teknologi jaringan komputer. Ketergantungan yang semakin besar terhadap teknologi jaringan komputer mengakibatkan penurunan kebutuhan akan keamanan yang memadai. Pelaku kejahatan siber dapat menggunakan setiap perangkat yang terhubung ke jaringan untuk mengeksploitasi kelemahan pada sistem.

Ancaman serangan siber di Indonesia terus meningkat dari tahun ke tahun. Berdasarkan data dari Badan Siber dan Sandi Negara (BSSN), terdapat puluhan juta anomali trafik yang terdeteksi setiap tahunnya, yang sebagian besarnya merupakan aktivitas malware dan trojan. Kondisi ini menunjukkan bahwa keamanan jaringan komputer bukan lagi sekadar kebutuhan teknis, melainkan telah menjadi kebutuhan strategis yang harus diprioritaskan oleh setiap organisasi.

Seiring dengan berkembangnya teknik serangan siber yang semakin canggih, tantangan untuk menjaga keamanan jaringan semakin sulit. Sistem pemerintah dan perusahaan besar bukan satu-satunya target pelaku kejahatan siber; mereka juga menargetkan lembaga pendidikan, usaha kecil menengah, dan bahkan individu. Serangan seperti Distributed Denial of Service (DDoS), brute force, SQL injection, dan penyebaran malware adalah ancaman yang paling umum bagi industri keamanan siber Indonesia.

Pemahaman yang mendalam tentang berbagai teknologi dan metodologi keamanan jaringan diperlukan untuk melindungi diri dari ancaman-ancaman tersebut. Untuk membangun ekosistem keamanan jaringan yang kokoh, beberapa elemen penting termasuk firewall, sistem deteksi intrusi (IDS), sistem pencegahan intrusi (IPS), Virtual Private Network (VPN), enkripsi, dan pengujian penetrasi. Faktor manusia dan kebijakan organisasi, selain elemen teknologi, sangat penting untuk menjaga integritas sistem.

Artikel ini disusun dengan tujuan untuk: (1) mengidentifikasi berbagai macam ancaman keamanan jaringan komputer yang umum terjadi di Indonesia; (2) mengkaji teknologi dan metode perlindungan jaringan yang telah dikembangkan dan diterapkan; (3) menganalisis efektivitas berbagai pendekatan keamanan berdasarkan hasil-hasil penelitian terdahulu; dan (4) memberikan rekomendasi strategis bagi organisasi dalam membangun sistem keamanan jaringan yang efektif dan berkelanjutan.

Urgensi kajian ini semakin diperkuat oleh fakta bahwa banyak organisasi di Indonesia, terutama institusi pendidikan dan pemerintahan daerah, masih memiliki infrastruktur keamanan jaringan yang belum memadai. Celah-celah keamanan yang ada sangat berpotensi dieksploitasi oleh pihak-pihak yang tidak bertanggung jawab, sehingga dapat mengakibatkan kebocoran data, gangguan layanan, hingga kerugian finansial yang signifikan.

1.1 Konsep Dasar Keamanan Jaringan Komputer

Keamanan jaringan komputer adalah serangkaian aturan, prosedur, dan mekanisme teknis yang digunakan untuk mencegah akses, penyalahgunaan, modifikasi, atau perusakan infrastruktur jaringan, data, dan sumber daya komputasi. Konsep ini terdiri dari tiga prinsip utama yang dikenal sebagai Triad CIA: Kerahasiaan (kerahasiaan), Integritas (integritas), dan Ketersediaan (ketersediaan). [1].

Prinsip kerahasiaan, atau kerahasiaan, mengacu pada keyakinan bahwa informasi hanya dapat diakses oleh pihak yang berwenang. Integritas (integritas) berarti memastikan bahwa data tidak mengalami perubahan ilegal selama proses penyimpanan atau transmisi. Namun, ketersediaan sistem dan data memastikan bahwa pengguna yang berhak dapat mengaksesnya pada saat dibutuhkan. Ketiga prinsip ini berfungsi sebagai dasar untuk desain dan evaluasi sistem keamanan jaringan. [2].

Ancaman keamanan jaringan dapat berasal dari berbagai sumber, baik internal maupun eksternal. Kesalahan pengguna, penyalahgunaan hak akses karyawan, dan kelalaian dalam prosedur keamanan adalah contoh ancaman internal. Sementara itu, ancaman eksternal mencakup serangan peretas, penyebaran malware, dan eksploitasi kerentanan sistem oleh pihak luar yang tidak memiliki otoritas. [3].

Selain itu, kerangka kerja keamanan jaringan yang menyeluruh juga mencakup elemen manajemen risiko, yang berarti bahwa organisasi harus menemukan, menilai, dan mengelola ancaman keamanan secara berkala. Metode seperti ini mencakup penilaian aset yang perlu dilindungi, pengenalan ancaman dan kerentanan, analisis dampak potensial, dan penetapan kontrol keamanan yang sesuai. [4]

1.2 Jenis-Jenis Ancaman Keamanan Jaringan

Seiring dengan kemajuan teknologi, ancaman keamanan jaringan komputer terus meningkat. Serangan Denial of Service (DDoS) adalah salah satu ancaman yang paling umum dan merusak. Pelaku melakukan DDoS dengan membanjiri server atau jaringan dengan lalu lintas data yang besar sehingga sistem tidak dapat menanggapi permintaan yang sah. Seperti yang ditunjukkan oleh penelitian [5], serangan DDoS dapat menyebabkan kerugian besar bagi bisnis dan membutuhkan sistem deteksi dan mitigasi yang canggih..

Serangan brute force adalah ketika pelaku mencoba berbagai kombinasi kata sandi hingga menemukan yang paling cocok. Spesifik, jenis serangan ini menyerang sistem autentikasi yang hanya menggunakan kata sandi sederhana atau tidak memiliki fitur yang membatasi percobaan login. Studi [6] menemukan bahwa kesalahan konfigurasi jaringan Wi-Fi dengan protokol WPA2-PSK dapat menyebabkan serangan brute force.

Malware terdiri dari virus, trojan, ransomware, worm, dan adware, dan dapat menyerang sistem melalui berbagai sumber serangan, seperti phishing email, unduhan dari situs berbahaya, atau perangkat USB yang terinfeksi. Sebagian besar anomali trafik jaringan di Indonesia disebabkan oleh aktivitas malware, menurut data BSSN yang dikutip dalam penelitian [7]. Ini menunjukkan betapa berbahayanya aktivitas malware bagi infrastruktur digital nasional.

Teknik serangan yang dikenal sebagai SQL Injection digunakan untuk mengubah query database dengan memasukkan kode SQL berbahaya melalui input pengguna yang tidak tervalidasi. Serangan ini dapat menyebabkan data sensitif bocor, diubah, atau dihapus, hingga orang lain mengambil kontrol sistem. [8] menyelidiki penggunaan IPS berbasis Suricata yang efektif untuk mengidentifikasi dan mencegah serangan SQL injection sebelum mencapai server database.

Ancaman terhadap kerahasiaan data yang ditransmisikan melalui jaringan termasuk sniffing dan serangan Man-in-the-Middle (MitM). Pelaku serangan ini berposisi di antara dua orang yang berbicara untuk menyadap atau mengubah data yang dikirim. [9] mempelajari cara menjalankan keamanan jaringan pada Mikrotik Router OS dengan menggunakan metode port knocking untuk memberikan perlindungan tambahan terhadap serangan seperti ini.

Serangan deauthentication pada jaringan Wi-Fi adalah ancaman yang memanfaatkan kelemahan protokol 802.11 untuk memutus koneksi perangkat dari point akses secara paksa. Studi yang menyelidiki kelemahan jaringan Wi-Fi di lingkungan kampus terhadap serangan jenis ini dan menyarankan penggunaan protokol WPA3 dan konfigurasi perlindungan frame manajemen (MFP) untuk mengurangi serangan ini [10].

1.3 Firewall sebagai Komponen Keamanan Utama

Dalam arsitektur keamanan jaringan, firewall adalah komponen pertahanan paling penting dan pertama. Sebagai penjaga gerbang, perangkat ini memantau dan menyaring lalu lintas jaringan sesuai dengan protokol keamanan . Untuk melindungi jaringan institusi pendidikan dari ancaman dari luar, firewall dipasang pada router Mikrotik. Hasilnya menunjukkan penurunan yang signifikan dalam jumlah trafik berbahaya yang masuk ke jaringan internal. [11]

[12] membuat perbandingan antara dua metode implementasi firewall, firewall filtering dan port blocking, pada infrastruktur jaringan skala menengah. Hasil penelitiannya menunjukkan bahwa menggunakan kombinasi kedua metode memberikan perlindungan yang lebih baik daripada menggunakan salah satu metode secara terpisah. Sementara firewall filtering memungkinkan kontrol yang lebih ketat terhadap konten lalu lintas, port blocking membantu mencegah akses ke layanan yang tidak diperlukan.

[13] mengusulkan model keamanan jaringan yang didasarkan pada firewall port blocking yang ditujukan untuk jaringan yang memiliki sumber daya terbatas. Efisiensi konfigurasi diutamakan sambil memberikan perlindungan yang cukup. Studi tersebut juga menekankan betapa pentingnya memperbarui ruleset firewall secara berkala untuk mengantisipasi ancaman baru.

[14] melakukan perbandingan kinerja sistem keamanan jaringan dengan firewall saja dibandingkan dengan kombinasi firewall dan VPN. Hasil penelitian

menunjukkan bahwa penggabungan VPN dan firewall memberikan perlindungan yang lebih baik, terutama untuk koneksi jarak jauh yang semakin populer di era kerja jarak jauh.

1.4 Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS)

IPS dan IDS adalah komponen keamanan jaringan yang bekerja sama dengan firewall. [15] melakukan analisis menyeluruh tentang seberapa baik kombinasi intrusion detection dan firewall melindungi jaringan komputer dari berbagai jenis serangan. Studi ini menemukan bahwa menggabungkan keduanya menghasilkan tingkat deteksi ancaman yang jauh lebih tinggi daripada menggunakan masing-masing bagian secara terpisah.

[16] menggabungkan Snort dengan Fail2Ban untuk menangani serangan brute force secara otomatis. Sistem ini menerima notifikasi secara real-time melalui Telegram, memungkinkan administrator jaringan untuk merespons masalah keamanan dengan lebih cepat. Hasil penggunaan menunjukkan bahwa metode ini berhasil menurunkan jumlah percobaan login ilegal yang berhasil mencapai server.

[17] menambahkan IPS berbasis Suricata ke jaringan institusi dan memeriksa kemampuan sistem untuk mendeteksi berbagai jenis serangan. Suricata, yang mendukung inspeksi paket multithreaded, terbukti dapat memproses trafik jaringan dengan kecepatan tinggi tanpa menimbulkan bottleneck yang signifikan. Oleh karena itu, itu cocok untuk digunakan pada jaringan yang memiliki banyak trafik.

[18] mengusulkan metode entropy untuk sistem deteksi serangan DDoS pada Software Defined Network (SDN). Pendekatan berbasis SDN memungkinkan deteksi dan respons terhadap serangan dilakukan secara terprogramatik dan lebih cepat dibandingkan metode konvensional karena controller SDN memiliki visibilitas global terhadap seluruh trafik jaringan.

1.5 Penetration Testing sebagai Metode Evaluasi Keamanan

Uji penetrasi, juga dikenal sebagai uji penetrasi, adalah teknik evaluasi keamanan jaringan yang mengidentifikasi kerentanan dalam sistem dengan mensimulasikan serangan nyata terhadap sistem. Ini dilakukan untuk mencegah pihak yang tidak bertanggung jawab mengeksploitasi kerentanan tersebut. [19] menggunakan metode pengujian penetrasi untuk melakukan pengujian kerentanan sistem. Metode ini berhasil menemukan banyak celah keamanan penting yang sebelumnya tidak diketahui oleh pengelola sistem.

[20] menggunakan teknik uji penetrasi untuk mengevaluasi keamanan jaringan berbasis Mikrotik dan menemukan beberapa kerentanan pada konfigurasi default yang dapat digunakan oleh penyerang. Penelitian ini menekankan betapa pentingnya konfigurasi hardening pada perangkat jaringan dan pembaruan firmware secara berkala untuk mencegah kerusakan.

[21] memanfaatkan alat analisis keamanan jaringan Kali Linux, terutama Nmap, Wireshark, dan Metasploit. Identifikasi port dan layanan yang terbuka, analisis trafik jaringan, dan eksploitasi kerentanan yang ditemukan dalam lingkungan pengujian yang terkontrol dapat dicapai dengan menggunakan kombinasi ketiga alat tersebut.

[2] menerapkan teknik pengujian penetrasi pada keamanan jaringan nirkabel dan mencatat secara sistematis seluruh proses pengujian mulai dari pencarian, pemindaian, pengoperasian, dan laporan. Metodologi yang terstruktur ini menghasilkan laporan keamanan yang lengkap dan dapat ditindaklanjuti yang dapat digunakan oleh pengelola jaringan.

[22] menggabungkan tes penetrasi dengan framework penilaian keamanan sistem informasi sekolah (ISSAF) untuk menilai keamanan jaringan sistem informasi sekolah. Rekomendasi untuk perbaikan yang lebih terstruktur dan evaluasi yang lebih menyeluruh dapat dicapai melalui penggabungan metode teknis dan kerangka kerja standar ini.

1.6 Port Knocking dan Teknik Perlindungan Akses

Teknik yang dikenal sebagai port knocking digunakan untuk melindungi jaringan dan menyembunyikan layanan dari pemindai port. Teknik ini menutup semua port secara otomatis dan hanya membuka akses setelah menerima sejumlah koneksi ke port tertentu dalam urutan yang tepat.

[23] menggunakan metode port knocking, yang telah terbukti efektif dalam menyembunyikan layanan SSH dari pemindaian port otomatis, yang biasa digunakan dalam fase awal serangan.

[24] meningkatkan keamanan port knocking dengan menggabungkan enkripsi asimetris RSA, yang berarti bahwa urutan ketukan port dienkripsi dan tidak dapat disadap oleh penyerang yang mengawasi trafik jaringan. Metode ini mengatasi kelemahan port knocking konvensional, yaitu rentan terhadap serangan replay jika penyerang dapat mencatat urutan ketukan, menggunakan kombinasi teknik knocking port dan blocking IP untuk melindungi server yang dimiliki oleh lembaga pemerintah dari serangan yang tidak sah. Menurut evaluasi implementasi, penerapan mekanisme keamanan berlapis ini mengurangi jumlah percobaan akses tidak sah yang berhasil mencapai server.

1.7 Keamanan Jaringan Nirkabel

Karena medium transmisinya yang tidak terbatas secara fisik, jaringan nirkabel menghadirkan tantangan keamanan yang berbeda. [25] Dengan menggunakan teknik penetration testing untuk memeriksa keamanan jaringan WLAN terhadap serangan brute force, kami menemukan bahwa banyak titik akses masih menggunakan konfigurasi keamanan yang buruk, terutama untuk kata sandi yang tidak memenuhi standar kompleksitas.

[26] memeriksa protokol keamanan Access 3 Protected Wi-Fi (WPA3) sebagai pengganti WPA2 yang lebih lama. Studi ini menunjukkan bahwa WPA3 meningkatkan keamanannya secara signifikan, terutama melalui mekanisme Simultaneous Authentication of Equals (SAE), yang lebih tahan terhadap serangan kata-kata dan kekuatan brute. Jika dibandingkan dengan mekanisme jabat tangan

WPA2, yang telah terbukti memiliki kelemahan, WPA3 menawarkan peningkatan keamanan yang lebih besar.
[27] membandingkan tiga metode pengujian keamanan jaringan WLAN: penetration testing standar, wardriving attack, dan metode SQUARE. Penelitian ini memberikan gambaran menyeluruh tentang vektor serangan yang mungkin dilakukan terhadap jaringan nirkabel dari berbagai sudut pandang, sehingga administrator jaringan dapat mempersiapkan pertahanan yang lebih menyeluruh.

1.8 Deteksi Malware dan Keamanan Protokol

[7] Analisis malware dinamis dan statis adalah dua pendekatan yang saling melengkapi yang digunakan untuk menganalisis dan mendeteksi malware pada protokol jaringan. Analisis dinamis melakukan malware dalam sandbox yang terisolasi untuk melacak perilakunya, sementara analisis statis memeriksa kode malware tanpa mengeksekusi. Menggabungkan kedua metode ini memberikan pemahaman yang lebih lengkap tentang ciri-ciri dan efek malware.
[28] Memanfaatkan HoneyPy dan Malicious Traffic Detection System (Maltrail) untuk mengidentifikasi serangan DoS pada server. Honeypot memungkinkan tim keamanan untuk mempelajari taktik penyerang tanpa mengancam sistem produksi, sementara Maltrail mendeteksi lalu lintas berbahaya berdasarkan daftar indikator kompromi yang selalu diperbarui.
[29] mengaktifkan Cloudflare Zero Trust untuk mengidentifikasi kejahatan cryptojacking yang terjadi pada jaringan komputer. Cryptojacking adalah ancaman baru di mana penyerang menyalahgunakan komputer korban untuk menambang mata uang kripto tanpa izin. Metode Zero Trust berhasil menemukan dan menghentikan tindakan mencurigakan.

1.9 Machine Learning untuk Keamanan Jaringan

Dalam sistem deteksi ancaman jaringan, pengajaran mesin memiliki potensi yang sangat besar untuk meningkatkan akurasi dan kecepatan deteksi. [30] mengklasifikasikan serangan DDoS berdasarkan karakteristik trafik jaringan dengan menggunakan algoritma Random Forest dan AdaBoost. Hasil penelitian menunjukkan bahwa metode pembelajaran kelompok ini dapat mendeteksi trafik DDoS dengan akurasi di atas 97% dibandingkan dengan trafik biasa.
[31] Mengusulkan metode rekayasa fitur berbasis machine learning yang dimaksudkan untuk mendeteksi serangan DDoS pada skala jaringan yang lebih besar. Penelitian ini menekankan betapa pentingnya memilih dan mengubah fitur yang tepat dari data trafik jaringan untuk meningkatkan kinerja model klasifikasi, terutama dalam menghadapi beragamnya serangan DDoS.

1.10 Framework dan Standar Keamanan Jaringan

Struktur dan standar keamanan yang diakui secara internasional memberi organisasi panduan sistematis untuk membangun dan mengevaluasi posisi keamanan jaringan mereka. [4] menerapkan NIST Cybersecurity Framework di universitas dan mendokumentasikan prosedur implementasinya. Dengan lima fungsi utamanya—Identify, Protect, Detect, Respond, dan Recover—Framework NIST menawarkan pendekatan yang menyeluruh untuk mengelola ancaman keamanan siber.
Dengan menggunakan switch port keamanan di simulator Cisco Packet Tracer, kami melihat keamanan jaringan komputer. Serangan MAC flooding dan koneksi perangkat yang tidak diizinkan adalah ancaman yang sering terjadi pada jaringan lokal berbasis kabel. Penggunaan switch port keamanan yang dikonfigurasi dengan benar dapat mencegah keduanya. [32].

2. METHODS

Pendekatan yang dipakai dalam riset ini ialah studi kepustakaan, tapi bukan sekadar kumpul-kumpul referensi biasa. Prosesnya cukup sistematis, penelusuran sumber dilakukan lewat beberapa basis data jurnal nasional seperti Google Scholar, Garuda alias Garba Rujukan Digital, dan SINTA. Rentang waktunya pun dibatasi, yakni artikel-artikel yang terbit antara 2021 sampai 2025, supaya data yang terjaring masih segar dan relevan dengan kondisi sekarang.
Kata kunci yang dipakai lumayan beragam. Mulai dari "keamanan jaringan", "firewall", "IDS/IPS", "penetration testing", "serangan DDoS", "brute force", "malware jaringan", "port knocking", hingga urusan "keamanan wireless" dan "enkripsi jaringan". Setelah artikel-artikel itu terkumpul, proses penyaringan dijalankan, bukan sembarangan. Aspek relevansi topik, kredibilitas si penerbit, sampai kelengkapan teks jadi tolok ukur utama yang dipakai.
Soal analisisnya, pendekatan kualitatif yang dikedepankan. Setiap sumber dibedah tema-tema utamanya, metodologi yang digunakan, apa saja temuan krusialnya, dan rekomendasi apa yang lahir dari kajian tersebut. Setelah itu baru dilakukan sintesis, alias proses mengintegrasikan berbagai temuan itu menjadi satu narasi yang padu. Tujuannya supaya ada gambaran menyeluruh soal arah perkembangan penelitian keamanan jaringan komputer di konteks Indonesia.
Dari penelusuran awal, lebih dari 80 artikel berhasil dijaring. Lumayan banyak, tapi tentu tidak semuanya lolos. Setelah disaring pakai kriteria inklusi-eksklusi yang sudah disusun sebelumnya, akhirnya 30 artikel terpilih sebagai sumber utama. Ke-30 artikel itu mewakili ragam subtopik keamanan jaringan yang kontekstual dan relevan dengan situasi di Indonesia.

3. RESULTS AND DISCUSSION

Dari 30 referensi yang sudah diseleksi, ada beberapa pola menarik yang muncul dari lanskap penelitian keamanan jaringan komputer di Indonesia selama lima tahun belakangan. Bukan pola yang mengejutkan, tapi cukup memberi gambaran jelas soal ke mana arah riset komunitas akademik kita.
Yang paling mencolok, dominasi penelitian berbasis Mikrotik itu nyata sekali. Platform ini jadi semacam "tanah bermain" favorit para peneliti lokal, dan wajar saja karena Mikrotik RouterOS memang sudah mengakar kuat di institusi pendidikan, kantor pemerintah daerah, sampai

segmen UKM. Penelitian-penelitian itu rata-rata bersifat terapan, menggabungkan konfigurasi teknis yang cukup rinci dengan evaluasi efektivitas yang terukur. Fokus utamanya berkutat di teknologi yang sudah mapan, firewall, IDS/IPS, sampai penetration testing.

Bicara soal penetration testing, metodologi ini menduduki posisi teratas sebagai pendekatan yang paling sering dipakai. Kadang jadi metode utama, kadang jadi bagian dari kerangka evaluasi yang lebih luas. Ini sinyal positif bahwa kesadaran komunitas riset Indonesia soal pentingnya pengujian keamanan secara proaktif, yang berbasis skenario serangan nyata, sudah mulai tumbuh.

Lalu ada tren lain yang lebih segar, pemanfaatan kecerdasan buatan dan machine learning dalam sistem deteksi ancaman. Jumlah penelitiannya memang masih kalah banyak dibanding yang konvensional, tapi kontribusi teknisnya justru lebih berbobot. Pendekatan Random Forest, deep learning, dan metode ensemble menunjukkan hasil yang lumayan menjanjikan buat klasifikasi serangan jaringan.

Keamanan jaringan nirkabel juga mendapat porsi perhatian yang cukup. Kerentanan terhadap serangan brute force dan deauthentication jadi fokus yang sering muncul. Transisi WPA2 ke WPA3 mulai disinggung dalam penelitian-penelitian terkini, walaupun adopsinya di lapangan masih jauh dari masif.

Satu catatan penting yang muncul dari kajian ini, Zero Trust Architecture dan cloud-based security hampir tidak kelihatan di literatur nasional yang dikaji. Kesenjangan ini cukup mencolok kalau dibandingkan dengan tren global. Tapi justru di situlah peluang besar terbuka untuk komunitas akademik Indonesia yang ingin berkontribusi pada sesuatu yang benar-benar belum banyak disentuh.

4. CONCLUSION

Kajian terhadap 30 referensi dari jurnal nasional terbitan 2021 hingga 2025 ini akhirnya melahirkan beberapa simpulan yang layak digarisbawahi, bukan sekadar rangkuman biasa. Soal ancaman, serangan DDoS, brute force, malware, dan SQL injection mendominasi perhatian para peneliti. Yang menarik, sasaran empuknya bukan hanya infrastruktur korporat besar, tapi justru institusi pendidikan, kantor pemerintah daerah, dan organisasi skala menengah yang sumber daya keamanannya jauh lebih terbatas. Ini ironi yang cukup menyedihkan sekaligus mendesak untuk ditangani.

Firewall masih jadi primadona. Paling banyak dikaji, paling banyak diimplementasikan. Berdampingan dengan itu, IDS/IPS berbasis open source macam Snort dan Suricata makin dikenal sebagai solusi yang efektif sekaligus ramah di kantong. Kombinasi keduanya dengan sistem notifikasi real-time lewat platform pesan instan, entah itu Telegram atau WhatsApp, kian populer sebagai metode monitoring yang praktis dan tidak ribet.

Penetration testing sudah naik kelas. Kalau dulu mungkin dianggap terlalu teknis atau eksklusif, sekarang metodologi ini diterima luas di komunitas peneliti Indonesia. Penggunaan tools seperti Kali Linux, Nmap, Wireshark, sampai Metasploit makin meluas, dan ini cerminan nyata dari peningkatan kapasitas teknis yang terjadi secara organik di lapangan.

Di sisi lain, machine learning mulai unjuk gigi. Algoritma ensemble seperti Random Forest dan AdaBoost memperlihatkan akurasi deteksi serangan yang cukup menggiurkan. Seiring bertambahnya ketersediaan dataset dan meningkatnya kapasitas komputasi para peneliti lokal, area ini diprediksi akan terus bergeliat.

Pada akhirnya, satu hal yang kajian ini tegaskan dengan cukup kuat yaitu keamanan jaringan bukan proyek sekali jadi. Butuh pendekatan berlapis, kombinasi teknologi yang pas, dan pembaruan yang tidak boleh berhenti karena ancaman pun tidak pernah berhenti berevolusi. Dan satu hal yang sering luput dari perhatian, investasi pada manusia, lewat pelatihan dan sertifikasi, sama strategisnya dengan investasi pada teknologi itu sendiri.

REFERENCES

[1] A. H. Harahap, C. D. Andani, A. Christie, D. Nurhaliza, and A. Fauzi, “Pentingnya peranan CIA Triad dalam keamanan informasi dan data untuk pemangku kepentingan atau stakeholder,” *J. Manaj. dan Pemasar. Digit.*, vol. 1, no. 2, pp. 73–83, 2023.

[2] N. A. Santoso, M. Ainurohman, and R. D. Kurniawan, “Penerapan metode penetration testing pada keamanan jaringan nirkabel,” *J Responsif Ris. Sains dan Inform.*, vol. 4, no. 2, pp. 162–167, 2022.

[3] M. I. Saputra, “Literature review network security,” *J. Jar. Komput. dan Keamanan*, vol. 4, no. 3, pp. 30–34, 2023, doi: 10.61346/jjkk.v4i3.66.

[4] T. Tan and B. Soewito, “Manajemen risiko serangan siber menggunakan framework NIST Cybersecurity di Universitas ZXC,” *J. Inf. Syst. Applied, Manag. Account. Res.*, vol. 6, no. 2, pp. 411–422, 2022, doi: 10.52362/jisamar.v6i2.781.

[5] N. Mamuriyah, S. E. Prasetyo, and A. O. Sijabat, “Rancangan sistem keamanan jaringan dari serangan DDoS menggunakan metode pengujian penetrasi,” *J. Teknol. dan Sist. Inf. Bisnis*, vol. 6, no. 1, pp. 162–167, 2024, doi: 10.47233/jteksis.v6i1.1124.

[6] S. Bahri, “Perancangan keamanan jaringan untuk mencegah terjadinya serangan bruteforce pada router,” *Indones. J. Educ. Comput. Sci.*, vol. 1, no. 3, pp. 136–147, 2023.

[7] V. R. Sianipar and H. Pangaribuan, “Analisis dan deteksi malware pada protokol jaringan menggunakan metode malware analisis dinamis dan malware analisis statis,” *Comput. Sci. Ind. Eng.*, vol. 9, no. 6, 2023.

[8] F. T. Anugrah and others, “Implementasi Intrusion Prevention System (IPS) menggunakan Suricata untuk serangan SQL injection,” *Techné J. Ilm.*

Elektrotek., vol. 21, p. 12, 2022.

[9] I. G. Raditya Putra, "Sejarah Artificial (Ai) Dan Fungsi Dalam Kehidupan Sehari Hari Pengantar Teknik Informatika Sejarah Artificial Intelligence (Ai) Dan," no. November, 2023.

[10] H. Handayani, K. U. Faizah, A. M. Ayulya, M. Fikri, and D. Wulan, "Jurnal Testing dan Implementasi Sistem Informasi PERANCANGAN SISTEM INFORMASI INVENTORY BARANG BERBASIS WEB MENGGUNAKAN METODE AGILE SOFTWARE DEVELOPMENT DESIGNING A WEB-BASED INVENTORY INFORMATION SYSTEM," vol. 1, no. 1, pp. 29–40, 2023.

[11] B. Cahya, F. Rizki, A. Sutiyo, Y. E. Saputra, and M. Elfarizi, "Implementasi firewall pada Mikrotik untuk keamanan jaringan," *JOCOTIS - J. Sci. Informatics Robot. \& Electron.*, vol. 1, no. 2, pp. 63–80, 2023.

[12] D. Wicaksono, "Firewall sistem keamanan jaringan menggunakan metode port blocking dan firewall filtering," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 2, pp. 1380–1392, 2022, doi: 10.35957/jatisi.v9i2.2103.

[13] S. Sartomo and W. Sulistyo, "Model keamanan jaringan menggunakan firewall port blocking," *Krea-TIF J. Tek. Inform.*, vol. 10, no. 1, pp. 10–18, 2022.

[14] F. S. Nabhan, S. N. Fahira, R. A. Syamputra, M. Farhan, and Saprudin, "Perbandingan kinerja sistem keamanan jaringan menggunakan firewall dan VPN," *Bul. Ilm. Ilmu Komput. dan Multimed.*, vol. 2, no. 5, pp. 910–913, 2025.

[15] Y. Mulyanto, E. S. Susanto, M. I. Akbar, and F. Idifitriani, "Analisis keamanan jaringan komputer menggunakan metode Intrusion Detection System (IDS) dan firewall," *Digit. Transform. Technol.*, vol. 3, no. 2, pp. 864–870, 2024, doi: 10.47709/digitech.v3i2.3402.

[16] R. K. Abdullah, M. Fudhail, and S. Mujahidin, "Penggunaan Snort dan Fail2Ban sebagai IDS untuk mengatasi brute force attack dengan notifikasi Telegram: Studi kasus pada institusi XYZ," *J. Sist. dan Teknol. Inf.*, vol. 12, no. 3, 2024, doi: 10.26418/justin.v12i3.79617.

[17] O. Rivaldi and N. L. Marpaung, "Penerapan sistem keamanan jaringan menggunakan Intrusion Prevention System berbasis Suricata," *Inovtek Polbeng - Seri Inform.*, vol. 8, no. 1, pp. 141–153, 2023.

[18] M. H. Hawarizmi, M. T. Kurniawan, and M. Fathinuddin, "Sistem deteksi serangan DDoS pada Software Defined Network menggunakan metode entropy," *SMART J. Sist. Inf.*, 2022.

[19] J. A. Ginting and I. G. G. N. Suryantara, "Pengujian kerentanan sistem dengan menggunakan metode penetration testing di Universitas XYZ," *Infotech J. Technol. Inf.*, vol. 7, no. 1, pp. 41–46, 2021, doi: 10.37365/jti.v7i1.105.

[20] A. Alfian, M. Purwaningsih, and F. D. N. Wicaksono, "Pencegahan kerentanan keamanan jaringan komputer Mikrotik menggunakan metode penetration testing," *J. Ilm. FIFO*, vol. 16, no. 2, p. 121, 2024, doi: 10.22441/fifo.2024.v16i2.003.

[21] A. Prana Walidin, F. P. Putri, and D. Kiswanto, "Kali Linux sebagai alat analisis keamanan jaringan melalui penggunaan Nmap, Wireshark, dan Metasploit," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 9, no. 1, pp. 1188–1196, 2024, doi: 10.36040/jati.v9i1.12661.

[22] E. P. Silmina, A. Firdonsyah, and R. A. A. Amanda, "Analisis keamanan jaringan sistem informasi sekolah menggunakan penetration test dan ISSAF," *Transmisi*, vol. 24, no. 3, pp. 83–91, 2022, doi: 10.14710/transmisi.24.3.83-91.

[23] D. Desmira and R. Wiryadinata, "Rancang bangun keamanan port Secure Shell (SSH) menggunakan metode port knocking," *J. Ilmu Komput. dan Sist. Inf.*, vol. 5, no. 1, pp. 28–33, 2022, doi: 10.55338/jikomsi.v5i1.242.

[24] Z. Amir, S. Syaifuddin, and D. Risqiwati, "Implementasi asymmetric encryption RSA pada port knocking Ubuntu Server menggunakan Knockd dan Python," *J. Teknol. Inf. Indones.*, 2022.

[25] R. Dayan, Y. Muhyidin, and D. Singasatia, "Analisis keamanan jaringan pada wireless local area network terhadap serangan brute force menggunakan metode penetration testing," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 7, no. 3, pp. 2051–2056, 2023, doi: 10.36040/jati.v7i3.7097.

[26] D. E. Faishol, T. A. Cahyanto, and M. Rahman, "Analisis dan evaluasi protokol keamanan jaringan nirkabel Wi-Fi Protected Access 3 dengan metode penetration testing," *J. Teknol. Inf.*, 2024.

[27] S. Hamza, N. H. Abri, and A. H. Muhammad, "Analisis keamanan jaringan wireless LAN menggunakan tiga metode penetration testing, wardriving attack, and SQUARE," *J. Ilm. Tek. Inform.*, 2023.

[28] H. Alfidzar and B. P. Zen, "Implementasi HoneyPy dengan Malicious Traffic Detection System (Maltrail) guna mendeteksi serangan DoS pada server," *J. Informatics, Inf. Syst. Softw. Eng. Appl.*,

vol. 4, no. 2, 2022.

[29] S. Adhar and U. Saprudin, “Implementasi Cloudflare Zero Trust dalam mendeteksi aktivitas cryptojacking pada jaringan komputer,” *J. Teknol. Komput. dan Sist. Inf.*, 2023.

[30] A. Fauzi and others, “Penerapan Random Forest dan Adaboost untuk klasifikasi serangan DDoS,” *J. Educ.*, vol. 5, no. 3, pp. 7925–7937, 2023.

[31] M. N. Faiz, O. Somantri, and A. W. Muhammad, “Rekayasa fitur berbasis machine learning untuk mendeteksi serangan DDoS,” *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 11, no. 3, 2022.

[32] A. Rahmatika, A. A. Manurung, and F. Ramadhani, “Analisis keamanan jaringan komputer dengan menggunakan switch port security di Cisco Packet Tracer,” *sudo J. Tek. Inform.*, vol. 2, no. 3, 2023.