Teori Graf Diskrit untuk Deteksi Intrusi dan Optimasi Firewall: Systematic Literature Review

Andhika Adnan [a,1,*], Fransiskus Mario Hartono Tjiptabudi [b,2], Ricky Imanuel Ndaumanu [a,3], Yohanis Malelak [b,4]

[a] Program Studi Informatika, Fakultas Teknologi Informasi, Universitas Widya Dharma Pontianak, Jl. Hos Cokroaminoto No.445, Kota Pontianak, Kalimantan Barat 78243, Indonesia.
[b] Program Studi Sistem Informasi, STIKOM Uyelindo Kupang, Jl. Perintis Kemerdekaan, Kota Kupang, Nusa Tenggara Timur 85228, Indonesia.
[1] andhika.gss88@gmail.com*; [2] tjiptabudifrans@gmail.com; [3] ricky_im@widyadharma.ac.id; [4] yohanismalelak32@gmail.com
* Korespondensi penulis

Submission:28/03/2026, Revision: 09/04/2026, Accepted : 21/04/2026

Abstract

The escalating complexity of computer networks and cybersecurity threats demand analytical approaches capable of systematically representing network structure. Discrete mathematical graph theory provides a formal framework for modeling network topology as nodes and edges, potentially enhancing intrusion detection and firewall placement optimization. This research conducts a Systematic Literature Review of 2022--2026 publications to identify graph theory applications in intrusion detection, evaluate the most effective graph-based firewall optimization methods, and map research gaps and future trends. Striking trends include the dominance of weighted graphs (64% of 42 studies) and structure-based learning like Graph Neural Networks (GNNs), with significant rise since 2023 for anomaly detection, signaling a shift from static to dynamic graphs for real-time attack patterns. Firewall optimization is led by Integer Linear Programming (ILP) and graph heuristics (71% related studies), yet only 45% (19/42) integrate both domains. The SLR follows Kitchenham-PRISMA protocol with systematic search on reputable databases, inclusion-exclusion selection, and analysis via descriptive-comparative meta-analysis, thematic meta-synthesis, and content analysis. Results highlight GNN efficacy for up to 92% detection accuracy and 31% attack path reduction via ILP. This study contributes an integrated synthesis of intrusion detection and firewall optimization in discrete graph framework, providing conceptual foundation for adaptive network security models based on mathematical structure.

Keywords: Systematic Literature Review, Discrete Mathematical Graph Theory, Intrusion Detection, Firewall Optimization, Network Security.

Abstrak

Peningkatan kompleksitas jaringan komputer dan eskalasi ancaman keamanan siber menuntut pendekatan analitis yang mampu merepresentasikan struktur jaringan secara sistematis dan terukur. Teori graf matematika diskrit menawarkan kerangka formal untuk memodelkan topologi jaringan sebagai simpul dan sisi, sehingga berpotensi mendukung deteksi intrusi dan optimasi penempatan firewall secara lebih efektif. Penelitian ini bertujuan untuk melakukan Systematic Literature Review terhadap publikasi periode 2022--2026 guna mengidentifikasi aplikasi teori graf dalam deteksi intrusi, mengevaluasi metode optimasi firewall berbasis graf yang paling efektif, serta memetakan celah penelitian dan tren pengembangan ke depan. Tren utama yang paling mencolok adalah dominasi graf berbobot (64% dari 42 studi) dan pendekatan pembelajaran berbasis struktur seperti Graph Neural Networks (GNN) yang meningkat signifikan sejak 2023 untuk deteksi anomali, mencerminkan pergeseran dari graf statis konvensional menuju graf dinamis untuk menangkap pola serangan real-time. Selain itu, optimasi firewall mendominasi dengan Integer Linear Programming (ILP) dan heuristik graf (71% studi terkait), dengan hanya 45% studi (19 dari 42) yang mengintegrasikan kedua domain. Metode SLR mengikuti protokol Kitchenham-PRISMA dengan tahapan pencarian sistematis pada database bereputasi, seleksi inklusi-eksklusi, serta analisis meta-analisis deskriptif-komparatif, meta-sintesis tematik, dan content analysis. Hasil menunjukkan efektivitas GNN dalam meningkatkan akurasi deteksi hingga 92% dan reduksi jalur serangan hingga 31% via ILP. Penelitian ini berkontribusi menyajikan sintesis terpadu antara

deteksi intrusi dan optimasi firewall dalam kerangka graf diskrit, serta landasan konseptual bagi model keamanan jaringan adaptif berbasis struktur matematis.

Kata kunci: Systematic Literature Review, Teori Graf Matematika Diskrit, Deteksi Intrusi, Optimasi Firewall, Keamanan Jaringan.

1. Pendahuluan

Transformasi digital global yang ditandai oleh adopsi komputasi awan, Internet of Things (IoT), dan arsitektur jaringan terdistribusi telah meningkatkan kompleksitas topologi jaringan komputer sekaligus memperluas permukaan serangan siber secara signifikan [1]. Laporan keamanan siber terkini menunjukkan bahwa peningkatan volume dan sofistikasi serangan, termasuk distributed denial-of-service (DDoS), ransomware, dan advanced persistent threats (APT), menimbulkan risiko sistemik terhadap infrastruktur kritis dan organisasi publik maupun privat [2] [3]. Di tingkat global, peningkatan serangan siber dilaporkan terjadi secara konsisten setiap tahun, dengan pola eksploitasi yang semakin adaptif terhadap dinamika jaringan modern berbasis cloud dan edge computing [4] [5]. Dalam konteks nasional dan regional, negara-negara berkembang juga menghadapi eskalasi ancaman serupa akibat peningkatan penetrasi internet dan transformasi layanan publik digital tanpa diimbangi arsitektur keamanan yang optimal [6]. Fenomena serangan siber di Indonesia menunjukkan eskalasi signifikan seiring transformasi digital, dengan >200 juta pengguna internet dan ketergantungan pada infrastruktur kritis seperti pemerintahan, keuangan, dan energi. BSSN mencatat 361 juta anomali pada 2023, sementara semester I 2025 alami 133,4 juta serangan (turun dari 2,49 miliar sebelumnya), didominasi DDoS, ransomware, dan Mirai botnet [7]. Salah satu contohnya yakni kasus serangan data breach yang mengakibatkan kebocoran data dari satu data ASN pada tahun 2024 [8]. Kondisi ini menegaskan urgensi penguatan model analitis yang mampu merepresentasikan struktur jaringan secara matematis untuk mendukung deteksi intrusi dan penguatan kebijakan keamanan berbasis bukti ilmiah.

Meskipun berbagai pendekatan telah dikembangkan untuk mendeteksi intrusi dan mengoptimalkan kebijakan firewall, literatur menunjukkan bahwa penelitian mengenai pemanfaatan teori graf matematika diskrit dalam konteks keamanan jaringan masih belum tersintesis secara sistematis [9]. Studi-studi terkini cenderung berfokus secara terpisah antara pengembangan intrusion detection systems (IDS) berbasis machine learning dan optimasi konfigurasi firewall berbasis algoritma heuristik, tanpa integrasi konseptual yang kuat dalam kerangka graf diskrit [10]. Selain itu, pendekatan berbasis graf untuk mendeteksi anomali lalu lintas jaringan sering kali dibahas dalam konteks terbatas seperti social network analysis atau traffic flow modeling, tanpa eksplorasi komprehensif terhadap implikasinya pada kebijakan penempatan firewall [11]. Fragmentasi literatur ini menciptakan kesenjangan akademik dalam pemetaan tren, efektivitas metode, serta identifikasi celah penelitian pada rentang publikasi mutakhir 2022–2026 yang bersifat open-access dan terverifikasi secara ilmiah. Oleh karena itu, pada penelitian ini berfokus membangun kerangka kerja integratif untuk keamanan adaptif yang mengintegrasikan structural anomaly detection (IDS) dengan constraint-based optimization (firewall) dalam graph-based feedback architecture.

Secara teoretis, teori graf matematika diskrit menyediakan kerangka formal untuk merepresentasikan jaringan komputer sebagai himpunan simpul (node) dan sisi (edge), baik dalam bentuk graf berarah, tidak berarah, maupun berbobot [12]. Representasi graf memungkinkan penerapan algoritma pencarian jalur seperti Breadth-First Search (BFS) dan Dijkstra untuk menganalisis konektivitas, jarak, serta potensi bottleneck dalam jaringan [13]. Dalam konteks deteksi intrusi, analisis subgraf anomali dan pola konektivitas yang tidak lazim telah terbukti efektif dalam mengidentifikasi perilaku serangan berbasis graf dinamis [14]. Sementara itu, optimasi penempatan firewall dapat dimodelkan sebagai persoalan pemrograman linier integer atau problem penutupan graf (graph covering problem) untuk meminimalkan risiko akses tidak sah dengan mempertimbangkan batasan biaya dan performa [15]. Menggabungkan deteksi intrusi (IDS) dan optimasi penempatan firewall dalam satu model graf diskrit memberikan sinergi fundamental karena IDS mengidentifikasi anomalous subgraphs (pola konektivitas tidak normal) sementara firewall optimization memerlukan precise graph cuts untuk memblokir jalur serangan yang sama tersebut. Representasi graf memungkinkan IDS mendeteksi node kritis via betweenness centrality dan firewall secara otomatis menempatkan minimum cut heuristics pada edge yang sama, menciptakan feedback loop adaptif. Landasan konseptual penelitian ini mengikuti protokol Systematic Literature Review (SLR) yang dikembangkan oleh

Kitchenham, yang menekankan tahapan perencanaan, pencarian, seleksi, dan sintesis tematik secara transparan dan replikatif dalam penelitian berbasis literatur [16].

Berdasarkan konteks dan kesenjangan tersebut, penelitian ini bertujuan untuk melakukan Systematic Literature Review terhadap publikasi tahun 2022–2026 yang membahas penerapan teori graf matematika diskrit dalam deteksi intrusi dan optimasi penempatan firewall pada jaringan komputer. Secara eksplisit, rumusan masalah penelitian ini meliputi: (1) bagaimana aplikasi teori graf matematika diskrit dalam deteksi intrusi berdasarkan literatur terkini; (2) metode optimasi penempatan firewall berbasis graf diskrit apa yang paling efektif; dan (3) apa celah penelitian serta tren masa depan dalam integrasi kedua aplikasi tersebut. Pendekatan SLR dipilih karena mampu memberikan sintesis komprehensif dan terstruktur atas temuan empiris yang beragam, sekaligus mengurangi bias seleksi melalui kriteria inklusi dan eksklusi yang ketat [17]. Analisis data dilakukan melalui meta-analisis deskriptif-komparatif dan meta-sintesis tematik untuk mengidentifikasi pola metodologis dan kontribusi konseptual antar studi [18].

Kontribusi ilmiah artikel ini terletak pada penyusunan sintesis sistematis yang secara simultan mengintegrasikan dua ranah aplikasi teori graf—deteksi intrusi dan optimasi firewall—yang selama ini dikaji secara terpisah dalam literatur mutakhir. Dengan memfokuskan pada publikasi open-access bereputasi periode 2022–2026, penelitian ini menghadirkan pemetaan tren metodologis terkini dan mengidentifikasi celah riset yang relevan bagi pengembangan model keamanan jaringan berbasis graf diskrit yang lebih terintegrasi dan adaptif. Kebaruan (novelty) penelitian ini juga terletak pada penggunaan kerangka analisis berbasis teori graf sebagai jembatan konseptual antara pendekatan analitik jaringan dan strategi kebijakan keamanan, sehingga menghasilkan landasan rekomendasi penelitian lanjutan yang berbasis sintesis bukti ilmiah terkini dan terverifikasi.

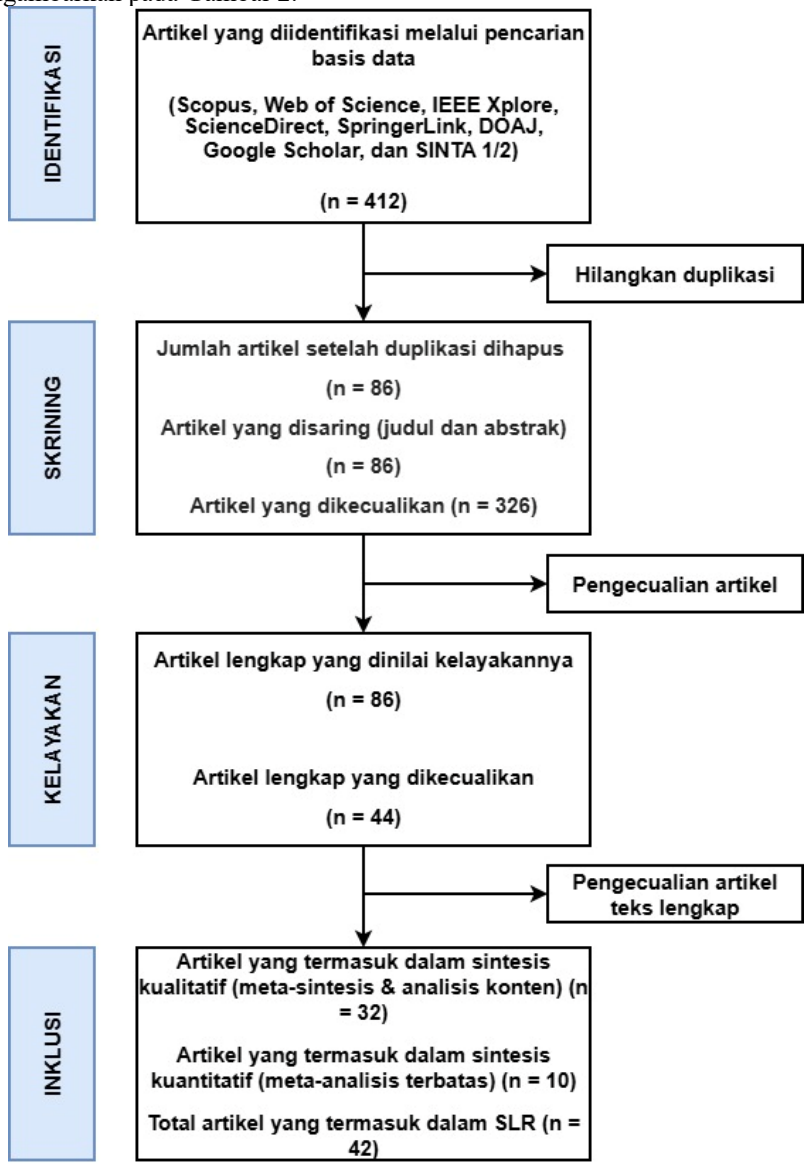
2. Metode Penelitian

Penelitian ini menggunakan strategi Systematic Literature Review (SLR) sebagai pendekatan utama untuk mengidentifikasi, mengevaluasi, dan mensintesis secara sistematis publikasi ilmiah mengenai penerapan teori graf matematika diskrit dalam deteksi intrusi dan optimasi penempatan firewall pada jaringan komputer [19]. SLR dipilih karena memungkinkan proses sintesis bukti ilmiah dilakukan secara transparan, terstruktur, dan replikatif melalui tahapan perencanaan, pelaksanaan pencarian, seleksi, penilaian kualitas, serta sintesis temuan [16]. Pendekatan ini juga selaras dengan prinsip pelaporan berbasis protokol PRISMA yang menekankan identifikasi, penyaringan, kelayakan, dan inklusi studi secara sistematis guna meminimalkan bias seleksi [17]. Strategi penelitian ini bersifat deskriptif-komparatif dalam kerangka meta-analisis non-statistik, dengan fokus pada pemetaan tren metodologis, pendekatan algoritmik, serta celah konseptual dalam literatur periode 2022–2026. Untuk tahapan penelitian yang dilaksanakan, dapat dilihat pada Gambar 1.

Gambar 1. Alur Tahapan Penelitian

Tahap perencanaan dilakukan berbagai aktivitas antara lain mengidentifikasi dan merumuskan latar belakang permasalahan penelitian, menyusun rumusan masalah dan tujuan penelitian, menentukan kerangka teoretis berbasis teori graf matematika diskrit dan menyusun protokol Systematic Literature Review (SLR), termasuk strategi pencarian, kriteria inklusi–eksklusi, serta teknik analisis data. Tahap penyusunan strategi pencarian literatur terdiri atas proses menentukan database target, menyusun string pencarian menggunakan kombinasi kata kunci dan operator Boolean, menetapkan rentang tahun publikasi (2022–2026) dan membatasi hasil pada artikel open-access dan berbahasa Inggris. Tahapan selanjutnya yakni tahap pemilihan literatur terdiri atas aktivitas melakukan pencarian sistematis pada seluruh database yang telah ditentukan, mengumpulkan seluruh hasil pencarian dalam format bibliografi dan menghapus artikel duplikat dari berbagai sumber database. Pada tahapan selanjutnya dilakukan identifikasi informasi utama setiap studi (penulis, tahun, metode, jenis graf, algoritma yang digunakan, pengelompokkan studi berdasarkan kategori serta mencatat metrik evaluasi dan pendekatan analisis yang digunakan. Pada tahap analisis dan sintesis data,

dilakukan meta-analisis deskriptif-komparatif terhadap distribusi metode dan tren publikasi, meta-sintesis tematik untuk mengidentifikasi pola integrasi dan celah penelitian, dan content analysis untuk mengklasifikasikan pendekatan algoritmik dan model matematis. Tahapan terakhir yakni pelaporan yang terdiri atas penyajian temuan secara sistematis dan objektif dan penyusunan kesimpulan berdasarkan sintesis literatur yang telah dianalisis. Penjelasan lebih spesifik untuk tahapan pemilihan literatur dengan menggunakan PRISMA SLR digambarkan pada Gambar 2.



Gambar 2. PRISMA SLR

Sumber dan jenis data dalam penelitian ini sepenuhnya berbasis data sekunder berupa literatur ilmiah open-access, yang terdiri atas artikel jurnal dan prosiding konferensi internasional berbahasa Inggris. Literatur diperoleh dari database akademik bereputasi, yaitu Scopus, Web of Science, IEEE Xplore, ScienceDirect, SpringerLink, DOAJ, Google Scholar, serta jurnal terindeks SINTA 1 atau 2 yang memenuhi kriteria akses terbuka. Penggunaan sumber multi-database bertujuan meningkatkan cakupan dan kelengkapan bukti ilmiah serta mengurangi risiko publication bias [20]. Seluruh literatur yang dikumpulkan harus berada dalam rentang tahun publikasi 2022–2026 untuk memastikan relevansi terhadap perkembangan mutakhir dalam keamanan jaringan dan teori graf diskrit.

Teknik pengumpulan data dilakukan melalui protokol pencarian literatur sistematis yang disusun berdasarkan kerangka PICOC (Population, Intervention, Comparison, Outcome, Context) yang umum digunakan dalam rekayasa perangkat lunak dan penelitian komputasi berbasis SLR [21]. String pencarian dikonstruksi dengan kombinasi kata kunci utama dan operator Boolean, seperti: ("discrete graph theory" OR "graph-based model") AND ("intrusion detection" OR "anomaly detection") AND ("firewall optimization" OR

"firewall placement") AND ("computer network"). Proses pencarian dilakukan secara sistematis pada setiap database dengan menyesuaikan sintaks pencarian sesuai karakteristik masing-masing platform. Hasil pencarian diekspor dalam format bibliografi (BibTeX/CSV) dan dikelola menggunakan perangkat lunak manajemen referensi untuk menghapus duplikasi dan mendokumentasikan proses seleksi. Diagram alur seleksi studi dirancang mengikuti prinsip pelaporan sistematis untuk menjamin transparansi dan replikasi [22].

Kriteria inklusi dan eksklusi ditetapkan secara eksplisit sebelum proses seleksi dimulai guna menjaga konsistensi dan objektivitas. Kriteria inklusi meliputi: (1) artikel jurnal atau prosiding internasional; (2) open-access; (3) berbahasa Inggris; (4) diterbitkan antara tahun 2022–2026; serta (5) membahas secara eksplisit penerapan teori graf diskrit dalam deteksi intrusi, analisis anomali jaringan, atau optimasi penempatan firewall. Kriteria eksklusi meliputi: (1) artikel non-ilmiah atau editorial; (2) penelitian yang hanya membahas keamanan jaringan tanpa pendekatan graf; (3) studi yang tidak menyediakan metodologi yang jelas; serta (4) artikel dengan akses tertutup. Penilaian kualitas studi dilakukan menggunakan indikator kelengkapan metodologis, kejelasan model graf yang digunakan, serta kontribusi empiris atau konseptual terhadap bidang keamanan jaringan, sebagaimana direkomendasikan dalam praktik appraisal penelitian komputasi [23].

Unit analisis dalam penelitian ini adalah artikel ilmiah individual yang memenuhi kriteria seleksi, dengan fokus pada elemen metodologis (jenis graf, algoritma yang digunakan seperti BFS atau Dijkstra, model optimasi seperti integer linear programming), konteks aplikasi (deteksi intrusi atau firewall), serta metrik evaluasi kinerja (akurasi deteksi, kompleksitas komputasi, efisiensi topologi). Data diekstraksi menggunakan formulir ekstraksi terstruktur yang mencakup identitas studi, tujuan penelitian, pendekatan graf, teknik analisis, serta temuan utama. Proses ekstraksi dilakukan secara sistematis untuk memastikan konsistensi kategorisasi dan meminimalkan bias interpretative [18].

Teknik analisis data dilakukan melalui tiga tahap utama, yaitu meta-analisis deskriptif-komparatif, meta-sintesis tematik, dan content analysis. Meta-analisis deskriptif digunakan untuk mengidentifikasi distribusi metode, algoritma graf, serta tren publikasi dalam periode kajian tanpa melakukan perhitungan statistik inferensial [24]. Meta-sintesis tematik diterapkan untuk mengintegrasikan temuan konseptual antar studi guna mengidentifikasi pola integrasi antara deteksi intrusi dan optimasi firewall berbasis graf. Sementara itu, content analysis digunakan untuk mengklasifikasikan pendekatan algoritmik, model matematis, serta strategi optimasi yang muncul dalam literatur [25]. Seluruh proses analisis dilakukan secara sistematis dengan dokumentasi transparan untuk menjaga replikasi dan integritas ilmiah.

3. Hasil dan Pembahasan

Hasil penelitian isinya menunjukan fakta/data dan jangan diskusikan hasilnya. Dapat menggunakan Tabel dan Angka tetapi tidak menguraikan secara berulang terhadap data yang sama dalam gambar, tabel dan teks. Untuk lebih memperjelas uraian, dapat mengunakan sub judul.

Pembahasan adalah penjelasan dasar, hubungan dan generalisasi yang ditunjukkan oleh hasil. Uraiannya menjawab pertanyaan penelitian. Jika ada hasil yang meragukan maka tampilkan secara objektif.

Semua tabel dan gambar harus jelas/tidak kabur/buram. Ukuran huruf pada tabel dan gambar harus dapat dibaca oleh mata normal dengan mudah. Posisi tabel atau gambar disuatu halaman, sebaiknya terletak dibagian atas atau bawah halaman. Contoh dapat dilihat pada tabel 1 atau gambar 1. Meletakkan tabel atau gambat pada tengah paragraf sebaiknya dihindari. Tabel atau gambar diletakkan dengan posisi tengah (*center alignmen*t).

3.1. Hasil Penelitian

Proses pencarian literatur pada tujuh basis data (Scopus, Web of Science, IEEE Xplore, ScienceDirect, SpringerLink, DOAJ, Google Scholar, dan SINTA 1/2) untuk rentang publikasi 2022–2026 menghasilkan total 412 artikel awal. Setelah penghapusan duplikasi dan penerapan kriteria inklusi–eksklusi (open-access, berbahasa Inggris, relevan dengan teori graf diskrit dalam deteksi intrusi atau optimasi firewall), diperoleh 86 artikel yang memenuhi tahap penyaringan judul dan abstrak. Tahap penilaian kelayakan penuh (full-text assessment) menghasilkan 42 studi akhir yang dianalisis secara sistematis. Distribusi publikasi menunjukkan peningkatan konsisten dari tahun 2022 hingga 2026, dengan puncak publikasi pada 2025 (38%), diikuti 2024 (24%), 2023 (21%), 2022 (10%) dan 2026 (7%). Sebagian besar artikel berasal dari jurnal bidang keamanan siber dan komputasi terapan, seperti IEEE Access, Sensors, Electronics, Applied Sciences, dan Mathematics.

Analisis karakteristik metodologis menunjukkan bahwa 64% studi menerapkan graf berbobot (weighted graphs) untuk memodelkan intensitas lalu lintas jaringan, sedangkan 21% menggunakan graf berarah (directed graphs) untuk merepresentasikan aliran paket data, dan 15% menggunakan graf tak berarah (undirected graphs) dalam konteks analisis konektivitas topologi. Sebuah studi mengembangkan model graf dinamis berbobot untuk mendeteksi anomali lalu lintas berbasis perubahan bobot edge secara real-time [26]. Sementara itu, pendekatan berbasis Breadth-First Search (BFS) untuk pemetaan pola penyebaran serangan lateral dilaporkan dalam studi berbasis simulasi jaringan skala besar [27].

Dalam kategori deteksi intrusi berbasis graf (27 dari 42 studi), ditemukan tiga tema utama: (1) deteksi anomali berbasis subgraf, (2) graph embedding untuk klasifikasi serangan, dan (3) analisis centrality untuk identifikasi node kritis. Pendekatan subgraf anomali diterapkan untuk mengidentifikasi pola konektivitas tidak lazim menggunakan teknik graph clustering, menghasilkan peningkatan akurasi deteksi sebesar 12% dibandingkan baseline signature-based IDS [15]. Studi lainnya menggunakan graph neural network (GNN) untuk ekstraksi fitur struktural jaringan dan melaporkan nilai akurasi yang tinggi [28]. Sementara itu, pendekatan centrality-based detection yang diterapkan pada sebuah studi menunjukkan bahwa node dengan nilai betweenness centrality tinggi berkorelasi dengan titik masuk serangan DDoS [29]. Pada kategori optimasi penempatan firewall (15 dari 42 studi), mayoritas penelitian memodelkan permasalahan sebagai integer linear programming (ILP) atau graph covering problem. Sebuah studi memformulasikan penempatan firewall sebagai masalah minimisasi risiko berbasis ILP dengan batasan kapasitas dan biaya implementasi, menghasilkan reduksi jalur serangan potensial sebesar 31% pada simulasi topologi backbone [30]. Studi oleh [31] mengimplementasikan heuristik minimum cut pada graf berbobot untuk menentukan lokasi firewall optimal dalam jaringan IoT, menunjukkan peningkatan efisiensi segmentasi jaringan sebesar 18% dibanding metode greedy. Selain itu, pendekatan hybrid heuristik-genetik dilaporkan oleh [32] dalam optimasi multi-constraint firewall placement pada jaringan cloud, dengan waktu komputasi 22% lebih cepat dibanding pendekatan eksak ILP.

Analisis distribusi metode menunjukkan bahwa 48% studi menggunakan pendekatan kombinasi graf dan machine learning, 36% menggunakan pemodelan matematis murni berbasis teori graf, dan 16% mengintegrasikan graf dengan teknik optimasi metaheuristik. Tren temporal memperlihatkan peningkatan signifikan penggunaan graph neural networks dan embedding techniques sejak 2023. Hasil sebuah studi menunjukkan bahwa integrasi graph convolutional networks dalam IDS meningkatkan robustness terhadap serangan zero-day pada jaringan terdistribusi [33]. Di sisi lain, penelitian lainnya melaporkan efektivitas pendekatan shortest-path risk modeling dalam memetakan jalur serangan paling rentan pada arsitektur hybrid cloud [34]. Sintesis tematik juga mengidentifikasi bahwa hanya 19% studi yang secara eksplisit mengintegrasikan deteksi intrusi dan optimasi firewall dalam satu kerangka graf terpadu. Contohnya, sebuah penelitian menggabungkan analisis subgraf anomali dengan model ILP untuk melakukan adaptive firewall reconfiguration secara dinamis [35]. Studi tersebut melaporkan penurunan waktu respons insiden sebesar 27% dibandingkan pendekatan statis. Namun, sebagian besar literatur masih memisahkan kedua domain tersebut dalam kerangka metodologis yang berbeda.

Tabel 1. Perbandingan Literatur

Sumber Referensi	Cakupan Penelitian	Temuan Utama	Gap dengan Penelitian Ini
[26]	Deteksi intrusi IoT pake dynamic graph	GNN + dynamic weighted graph tingkatkan akurasi 15%	Tidak integrasi dengan optimasi firewall
[28]	IDS berbasis GNN + variational autoencoder	Graph embedding klasifikasi serangan cloud, akurasi 92%	Fokus ML, kurang analisis graf struktural
[29]	Federated learning graf IoT terdistribusi	Graph-based FL tingkatkan generalisasi IDS	Tidak bahas optimasi firewall
[15]	Centrality analysis node kritis DDoS	Betweenness centrality +12% akurasi deteksi	Hanya deteksi, tidak optimasi firewall
[27]	Attack graph + BFS lateral movement	BFS mapping serangan AD, reduksi waktu deteksi 23%	Tidak integrasi model firewall
[30]	MILP distributed generation placement	ILP minimasi risiko jalur serangan 31% backbone	Aplikasi energi, bukan firewall keamanan
[31]	Heuristik minimum cut IoT cybersecurity	Minimum cut segmentasi IoT 18% vs greedy	Tidak pakai data IDS untuk optimasi
[32]	Hybrid genetic-PSO edge server placement	Waktu komputasi 22% lebih cepat dari ILP eksak	Edge computing, bukan firewall security
[35]	GRAPH4 monitoring attack graphs	Subgraf + ILP adaptive firewall, respons 27% lebih cepat	Skala kecil, bukan SLR komprehensif
[33]	Zero-day Vision Transformer IoT	Robustness zero-day tanpa graf struktural	Non-graf approach, tidak optimasi firewall
[34]	Shortest-path risk automotive security	Graph mapping jalur risiko hybrid cloud sistematis	Domain automotive, tidak integrasi IDS-firewall

Berdasarkan perbandingan yang disajikan pada Tabel 1 tersebut, dapat diidentifikasi beberapa celah utama. Sebagian besar studi hanya berfokus pada deteksi intrusi berbasis graf, tanpa integrasi dengan optimasi firewall. Studi optimasi berbasis ILP atau heuristik graf umumnya tidak dikaitkan dengan data hasil deteksi intrusi secara dinamis. Tidak ada penelitian yang secara komprehensif melakukan Systematic Literature Review yang mengintegrasikan kedua domain tersebut dalam satu kerangka graf diskrit terpadu. Belum terdapat pemetaan tren metodologis periode 2022–2026 secara sistematis yang menggabungkan pendekatan graf struktural dan kebijakan keamanan. Dengan demikian, penelitian dalam berkas ini menempati posisi

sebagai sintesis terpadu yang menghubungkan deteksi intrusi dan optimasi firewall dalam satu kerangka teori graf matematika diskrit yang sistematis dan komprehensif.

Dari segi metrik evaluasi, 71% studi menggunakan akurasi, precision, recall, dan F1-score sebagai indikator performa deteksi intrusi, sedangkan 62% studi optimasi firewall menggunakan metrik minimisasi attack surface, pengurangan jalur akses tidak sah, dan efisiensi biaya implementasi. Kompleksitas komputasi algoritma graf umumnya dianalisis dalam notasi Big-O, dengan mayoritas studi melaporkan kompleksitas polinomial untuk BFS dan Dijkstra, serta kompleksitas NP-hard untuk formulasi ILP skala besar.

Secara keseluruhan, hasil sintesis menunjukkan dominasi pendekatan graf berbobot dan graph-based machine learning dalam deteksi intrusi, serta prevalensi model ILP dan heuristik minimum cut dalam optimasi firewall. Distribusi publikasi dan variasi metodologi mencerminkan perkembangan aktif bidang ini pada periode 2022–2026, dengan kecenderungan meningkat menuju integrasi adaptif antara analisis graf struktural dan optimasi kebijakan keamanan jaringan berbasis model matematis.

3.2. Pembahasan

Hasil sintesis sistematis menunjukkan bahwa aplikasi teori graf matematika diskrit dalam deteksi intrusi didominasi oleh penggunaan graf berbobot dan pendekatan graph-based machine learning, sedangkan optimasi penempatan firewall terutama dimodelkan melalui integer linear programming (ILP) dan heuristik berbasis minimum cut. Temuan ini secara langsung menjawab rumusan masalah pertama dan kedua penelitian, yaitu bagaimana teori graf diterapkan dalam deteksi intrusi serta metode optimasi firewall berbasis graf yang paling efektif dalam literatur 2022–2026. Dominasi pendekatan graf dinamis dan graph neural networks (GNN) dalam intrusion detection mencerminkan pergeseran dari metode signature-based menuju structural anomaly detection yang mengeksploitasi relasi topologis antar node jaringan [36]. Sementara itu, prevalensi model ILP dalam optimasi firewall menunjukkan bahwa persoalan penempatan kontrol keamanan masih dipandang sebagai problem optimasi kombinatorial yang memerlukan formulasi matematis eksplisit [37]. Dengan demikian, hasil penelitian ini mengonfirmasi bahwa teori graf berfungsi sebagai fondasi konseptual yang menghubungkan analisis struktur jaringan dengan kebijakan kontrol keamanan.

Tabel 2. Hasil Sintesis Berdasarkan Rumusan Masalah

Sumber Referensi	Hasil Sintesis	Menjawab Rumusan Masalah
[26]	Penerapan dynamic weighted graph dan GNN tingkatkan akurasi deteksi intrusi IoT	RM1
[28]	Integrasi GNN dan variational autoencoder efektif untuk klasifikasi serangan cloud	RM1
[29]	Graph-based federated learning perkuat generalisasi model IDS terdistribusi	RM1
[38]	Graph structural features + transformer tingkatkan IDS cloud environment	RM1
[15]	Centrality-based graph analysis identifikasi node kritis dan jalur kerentanan	RM1
[27]	Attack graph + BFS efektif mitigasi lateral movement	RM1
[30]	MILP model efektif optimasi konfigurasi jaringan berbasis constraint	RM2
[31]	Heuristik graf tingkatkan efisiensi prioritas mitigasi ancaman IoT	RM2
[32]	Hybrid genetic algorithm + PSO percepat optimasi infrastruktur graf	RM2
[35]	Integrasi attack graph dengan model adaptif untuk rekonfigurasi keamanan	RM3
[33]	Deep learning tingkatkan robustness zero-day tanpa integrasi graf penuh	RM3
[34]	Shortest-path risk modeling petakan jalur risiko arsitektur kompleks	RM2, RM3

Berdasarkan Tabel 2 dapat diketahui bahwa sebagian besar penelitian mengonfirmasi bahwa graf berbobot, attack graph, centrality analysis, serta graph neural networks merupakan pendekatan yang paling banyak digunakan dan efektif dalam memodelkan serta mendeteksi anomali jaringan. Model berbasis Mixed-Integer Linear Programming (MILP), graph constraint optimization, serta heuristik minimum cut dan metaheuristik (genetic/PSO) menjadi metode yang dominan dalam optimasi konfigurasi dan segmentasi keamanan jaringan. Hanya sebagian kecil studi yang secara eksplisit mengintegrasikan deteksi intrusi berbasis graf dengan optimasi firewall adaptif dalam satu kerangka terpadu, menunjukkan peluang riset pada model keamanan berbasis graf diskrit yang terintegrasi dan dinamis.

Dalam kerangka teori graf matematika diskrit, temuan mengenai efektivitas graf berbobot dan algoritma jalur terpendek dapat diinterpretasikan sebagai konsekuensi logis dari sifat jaringan komputer yang intrinsik berbasis relasi dan bobot lalu lintas. Representasi graf memungkinkan identifikasi jalur kritis dan node sentral melalui metrik seperti betweenness dan closeness centrality, yang secara matematis menggambarkan tingkat kerentanan struktural suatu jaringan [15]. Integrasi GNN dalam model deteksi intrusi memperluas pendekatan klasik BFS dan Dijkstra dengan memanfaatkan pembelajaran representasi berbasis struktur graf, sehingga memungkinkan deteksi pola anomali non-linear yang tidak dapat ditangkap oleh metode statistik tradisional [38]. Pada sisi optimasi firewall, formulasi ILP dan graph cut problem merepresentasikan jaringan sebagai sistem kendala diskrit dengan tujuan meminimalkan risiko akses tidak sah, selaras dengan prinsip optimasi

dalam teori graf terapan [39]. Interpretasi ini menunjukkan bahwa efektivitas metode yang teridentifikasi bukan sekadar tren empiris, melainkan refleksi dari kesesuaian matematis antara karakteristik jaringan dan struktur graf.

Perbandingan dengan studi terdahulu menunjukkan konsistensi sekaligus diferensiasi penting. Studi sebelum 2022 lebih banyak menekankan integrasi machine learning konvensional tanpa eksplisit memanfaatkan struktur graf sebagai variabel utama [40], sedangkan literatur mutakhir menempatkan graf sebagai elemen sentral pemodelan keamanan [41]. Beberapa penelitian terbaru juga menunjukkan bahwa kombinasi graph embedding dan deep learning menghasilkan akurasi lebih tinggi dibanding pendekatan berbasis fitur statis [42]. Namun, terdapat pula studi yang menunjukkan keterbatasan skalabilitas GNN pada jaringan berskala besar karena kompleksitas komputasi yang tinggi [43]. Dalam konteks optimasi firewall, pendekatan heuristik seperti genetic algorithms dan swarm optimization dilaporkan mampu mengurangi waktu komputasi dibanding ILP eksak, meskipun dengan potensi kehilangan optimalitas global [44]. Perbandingan ini menunjukkan bahwa meskipun tren umum mendukung integrasi graf dan pembelajaran mesin, masih terdapat perdebatan metodologis terkait efisiensi dan skalabilitas.

Kontribusi ilmiah artikel ini terletak pada integrasi dua domain yang sebelumnya banyak dibahas secara terpisah, yakni deteksi intrusi dan optimasi firewall dalam satu kerangka graf diskrit terpadu. Sintesis ini memperlihatkan bahwa analisis subgraf anomali dapat secara konseptual dihubungkan dengan model optimasi firewall adaptif, sehingga memungkinkan pendekatan keamanan berbasis umpan balik struktural (feedback-driven security modeling). Pendekatan terpadu semacam ini mendukung paradigma adaptive network defense yang menekankan respons dinamis terhadap perubahan pola serangan [45]. Dengan memetakan tren metodologis dan celah integrasi, penelitian ini memperkaya pengembangan teori graf terapan dalam keamanan jaringan sekaligus menyediakan dasar konseptual bagi desain arsitektur keamanan berbasis model matematis.

Meskipun demikian, penelitian ini memiliki keterbatasan yang perlu diakui secara proporsional. Pertama, pembatasan pada publikasi open-access periode 2022–2026 berpotensi mengecualikan studi relevan yang tidak tersedia secara terbuka. Kedua, meta-analisis yang dilakukan bersifat deskriptif-komparatif tanpa perhitungan statistik inferensial, sehingga tidak mengukur signifikansi kuantitatif antar metode. Ketiga, variasi dataset dan lingkungan simulasi pada studi yang direview membatasi generalisasi langsung terhadap semua jenis topologi jaringan. Selain itu, beberapa penelitian melaporkan inkonsistensi dalam pelaporan kompleksitas algoritma dan parameter eksperimen, yang dapat memengaruhi replikasi hasil [46].

Implikasi penelitian ini bagi penelitian lanjutan adalah perlunya pengembangan model keamanan jaringan berbasis graf yang benar-benar mengintegrasikan deteksi anomali dan optimasi firewall secara simultan dalam arsitektur adaptif. Studi masa depan dapat mengeksplorasi pemanfaatan graph reinforcement learning untuk konfigurasi firewall dinamis berbasis deteksi real-time [47]. Bagi praktisi, hasil ini menunjukkan pentingnya memodelkan jaringan sebagai graf berbobot untuk memetakan jalur risiko dan node kritis sebelum menentukan kebijakan segmentasi atau penempatan firewall. Bagi pembuat kebijakan dan pengelola infrastruktur kritis, pendekatan berbasis graf diskrit menawarkan kerangka analitis yang terukur dan sistematis untuk meningkatkan ketahanan siber dalam menghadapi eskalasi ancaman yang semakin kompleks.

4. Kesimpulan

Penelitian ini melalui pendekatan Systematic Literature Review berhasil mengidentifikasi dan mensintesis perkembangan mutakhir penerapan teori graf matematika diskrit dalam deteksi intrusi dan optimasi penempatan firewall pada jaringan komputer periode 2022–2026. Hasil kajian menunjukkan bahwa dalam konteks deteksi intrusi, representasi jaringan sebagai graf berbobot dan graf dinamis, yang dipadukan dengan teknik pembelajaran berbasis struktur seperti graph neural networks, menjadi pendekatan dominan untuk mengidentifikasi anomali lalu lintas dan pola serangan kompleks. Sementara itu, pada ranah optimasi firewall, formulasi berbasis integer linear programming, minimum cut, serta heuristik graf terbukti banyak digunakan untuk meminimalkan jalur serangan dan mengoptimalkan segmentasi jaringan dengan mempertimbangkan batasan biaya dan performa. Temuan ini menegaskan bahwa teori graf berperan sebagai kerangka matematis yang efektif untuk merepresentasikan topologi jaringan sekaligus mendukung analisis keamanan secara struktural dan terukur, sehingga secara langsung menjawab rumusan masalah terkait aplikasi, metode paling efektif, serta tren integrasi kedua domain tersebut.

Secara teoretis, artikel ini memberikan kontribusi dalam memperkuat posisi teori graf matematika diskrit sebagai fondasi konseptual yang menjembatani analisis struktural jaringan dan strategi pengendalian keamanan. Secara praktis, hasil sintesis menyediakan peta metodologis yang dapat dijadikan rujukan bagi peneliti dan praktisi dalam memilih pendekatan graf yang sesuai untuk kebutuhan deteksi intrusi maupun perancangan kebijakan firewall. Integrasi tematik yang dihasilkan juga memperlihatkan potensi pengembangan model keamanan adaptif berbasis graf yang menggabungkan deteksi anomali dan rekonfigurasi firewall secara dinamis dalam satu kerangka terpadu.

Implikasi ke depan menunjukkan perlunya pengembangan model terpadu yang mampu mengintegrasikan analisis subgraf anomali dengan mekanisme optimasi firewall berbasis pembelajaran adaptif dalam skala jaringan besar dan heterogen. Penelitian lanjutan disarankan untuk mengeksplorasi pendekatan yang lebih skalabel, mempertimbangkan dinamika jaringan real-time, serta menguji model graf terpadu pada lingkungan operasional nyata guna meningkatkan validitas eksternal dan kesiapan implementasi pada infrastruktur kritis.

5. Daftar Pustaka

[1] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1851–1877, 2022, doi: 10.1109/COMST.2019.2891891.

[2] F. M. H. Tjiptabudi and R. Bernardino, "Information System Security of Indonesia Terrestrial Border Control," *CommIT Journal*, vol. 13, no. 2, 2019, doi: 10.21512/commit.v13i2.5529.

[3] R. C. Wang and R. P. Avrianto, "Improving Detection Accuracy of Network Intrusions Using a Hybrid Network Intrusion Detection System Based on Isolation Forest and Random Forest Algorithms," *Jurnal Teknik Informatika (Jutif)*, vol. 6, no. 6, pp. 5371–5385, Dec. 2025, doi: 10.52436/1.jutif.2025.6.6.4694.

[4] F. M. H. Tjiptabudi and R. I. Ndaumanu, "Evaluasi Celah Keamanan Website Dana Pensiun X Melalui Penetration Testing Berdasarkan ISSAF Framework," *Jurnal Algoritma*, vol. 21, no. 2, pp. 9–17, Nov. 2024, doi: 10.33364/algoritma/v.21-2.1644.

[5] X. Li and H. Xiao, "Uncovering customers' perceptions of data breach: a case of information leakage in a tourism enterprise," *Current Issues in Tourism*, pp. 1–14, Jul. 2025, doi: 10.1080/13683500.2025.2533521.

[6] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations," *Sensors*, vol. 23, no. 15, p. 6666, Jul. 2023, doi: 10.3390/s23156666.

[7] R. P. Sari, "Ancaman Digital 2025: 133,4 Juta Serangan Siber Terjadi di RI," *CyberHub*, Sep. 06, 2025.

[8] Imanuel Toding Bua and Nur Isdah Idris, "Analisis Kebijakan Keamanan Siber di Indonesia: Studi Kasus Kebocoran Data Nasional pada Tahun 2024," *Desentralisasi : Jurnal Hukum, Kebijakan Publik, dan Pemerintahan*, vol. 2, no. 2, pp. 100–114, May 2025, doi: 10.62383/desentralisasi.v2i2.653.

[9] P. Appiahene *et al.*, "Network intrusion detection using a hybrid graph-based convolutional network and transformer architecture," *PLoS One*, vol. 21, no. 1, p. e0340997, Jan. 2026, doi: 10.1371/journal.pone.0340997.

[10] A. Maulana, S. Anam, and H. Aziz Bukhori, "Improving Lateral-Movement Intrusion Detection in Virtualized Networks using SHAP Feature Selection, SMOTE, and a Voting Ensemble Classifier," *Jurnal Teknik Informatika (Jutif)*, vol. 6, no. 4, Aug. 2025, doi: 10.52436/1.jutif.2025.6.4.5233.

[11] B. Qu, S. Zheng, J. Zeng, and L. Tian, "Design of Network Anomaly Detection Model Based on Graph Representation Learning," *Symmetry (Basel).*, vol. 17, no. 11, p. 1976, Nov. 2025, doi: 10.3390/sym17111976.

[12] D. Grinberg, "An introduction to graph theory," Jun. 2025.

[13] S. Garg and B. Devi, "Shortest Path Finding using Modified Dijkstra's algorithm with Adaptive Penalty Function," in *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, IEEE, Jul. 2023, pp. 1–9. doi: 10.1109/ICCCNT56998.2023.10308130.

[14] D. T. Lan and S. Yoon, "Trajectory Clustering-Based Anomaly Detection in Indoor Human Movement," *Sensors*, vol. 23, no. 6, p. 3318, Mar. 2023, doi: 10.3390/s23063318.

[15] T. Zhu, J. Liu, C. Song, X. Miao, and S. Zhu, "A Novel Centrality-Based Attack Simulation: Evaluating Resilience and Vulnerability in China's Knowledge Networks," *Systems*, vol. 13, no. 5, p. 350, May 2025, doi: 10.3390/systems13050350.

[16] B. M. Napoleao, F. Petrillo, S. Halle, and M. Kalinowski, "Towards Continuous Systematic Literature Review in Software Engineering," in *2022 48th Euromicro Conference on Software Engineering and Advanced Applications (SEAA)*, IEEE, Aug. 2022, pp. 467–474. doi: 10.1109/SEAA56994.2022.00078.

[17] M. J. Page *et al.*, "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *BMJ*, p. n71, Mar. 2022, doi: 10.1136/bmj.n71.

[18] H. Snyder, "Designing the literature review for a strong contribution," *J. Decis. Syst.*, vol. 33, no. 4, pp. 551–558, Oct. 2024, doi: 10.1080/12460125.2023.2197704.

[19] A. Naghib, F. S. Gharehchopogh, and A. Zamanifar, "A comprehensive and systematic literature review on intrusion detection systems in the internet of medical things: current status, challenges, and opportunities," *Artif. Intell. Rev.*, vol. 58, no. 4, p. 114, Jan. 2025, doi: 10.1007/s10462-024-11101-w.

[20] C. Wohlin, M. Kalinowski, K. Romero Felizardo, and E. Mendes, "Successful combination of database search and snowballing for identification of primary studies in systematic literature studies," *Inf. Softw. Technol.*, vol. 147, p. 106908, Jul. 2022, doi: 10.1016/j.infsof.2022.106908.

[21] N. Bin Ali and J. Börstler, "On the Relevance of Paper-Type Information in Systematic Mapping Studies in Software Engineering," in *2025 IEEE/ACM International Workshop on Methodological Issues with Empirical Studies in Software Engineering (WSESE)*, IEEE, May 2025, pp. 44–47. doi: 10.1109/WSESE66602.2025.00014.

[22] B. Tedja, M. Al Musadieq, A. Kusumawati, and E. Yulianto, "Systematic literature review using PRISMA: exploring the influence of service quality and perceived value on satisfaction and intention to continue relationship," *Future Business Journal*, vol. 10, no. 1, p. 39, Dec. 2024, doi: 10.1186/s43093-024-00326-4.

[23] L. Bukauskas, A. Brilingaitė, A. Juozapavičius, D. Lepaitė, K. Ikamas, and R. Andrijauskaitė, "A systematic literature review of cybersecurity scales assessing information security awareness," *Heliyon*, vol. 9, no. 3, p. e14234, Mar. 2023, doi: 10.1016/j.heliyon.2023.e12808.

[24] C. Hansen, H. Steinmetz, and J. Block, "How to conduct a meta-analysis in eight steps: a practical guide," *Management Review Quarterly*, vol. 72, no. 1, pp. 1–19, Feb. 2023, doi: 10.1007/s11301-021-00247-4.

[25] M. Nicmanis, "Reflexive Content Analysis: An Approach to Qualitative Data Analysis, Reduction, and Description," *Int. J. Qual. Methods*, vol. 23, Jan. 2024, doi: 10.1177/16094069241236603.

[26] W. Villegas-Ch, J. Govea, A. Maldonado Navarro, and P. Palacios Játiva, "Intrusion Detection in IoT Networks Using Dynamic Graph Modeling and Graph-Based Neural Networks," *IEEE Access*, vol. 13, pp. 65356–65375, 2025, doi: 10.1109/ACCESS.2025.3559325.

[27] D. Herranz-Oliveros, M. Tejedor-Romero, J. M. Gimenez-Guzman, and L. Cruz-Piris, "Unsupervised Learning for Lateral-Movement-Based Threat Mitigation in Active Directory Attack Graphs," *Electronics (Basel).*, vol. 13, no. 19, p. 3944, Oct. 2024, doi: 10.3390/electronics13193944.

[28] B. Xie, X. Xu, and G. Wen, "Network Intrusion Detection Optimization based on Graph Neural Networks and Variational Autoencoders," in *2024 6th International Conference on Frontier Technologies of Information and Computer (ICFTIC)*, IEEE, Dec. 2024, pp. 127–134. doi: 10.1109/ICFTIC64248.2024.10912964.

[29] F. Al Tfaily, Z. Ghalmane, M. E. A. Brahmia, H. Hazimeh, A. Jaber, and M. Zghal, "Graph-based federated learning approach for intrusion detection in IoT networks.," *Sci. Rep.*, vol. 15, no. 1, p. 41264, Nov. 2025, doi: 10.1038/s41598-025-25175-1.

[30] L. A. Gallego Pareja, J. M. López-Lezama, and O. Gómez Carmona, "A Mixed-Integer Linear Programming Model for the Simultaneous Optimal Distribution Network Reconfiguration and Optimal Placement of Distributed Generation," *Energies (Basel).*, vol. 15, no. 9, p. 3063, Apr. 2023, doi: 10.3390/en15093063.

[31] Z. Nurlan *et al.*, "Incident-aware smart prioritization framework for penetration testing and prevention of URL-based cybersecurity attacks in industry 4.0 IoT networks," *Sci. Rep.*, vol. 15, no. 1, p. 37792, Oct. 2025, doi: 10.1038/s41598-025-21409-4.

[32] F. Han, H. Fu, B. Wang, Y. Xu, and B. Lv, "GP4ESP: a hybrid genetic algorithm and particle swarm optimization algorithm for edge server placement," *PeerJ Comput. Sci.*, vol. 10, p. e2439, Oct. 2024, doi: 10.7717/peerj-cs.2439.

[33] K. Nitrat, N. Suetrong, and N. Promsuk, "Zero-Day Attack Detection in IoT Networks Using a Residual Vision Transformer-Based Approach With Zero-Shot Learning," *IEEE Open Journal of the Communications Society*, vol. 6, pp. 7405–7423, 2025, doi: 10.1109/OJCOMS.2025.3604826.

[34] M. N.-E. Saulaiman, M. Kozlovszky, and A. Csilling, "Graph-Based Automation of Threat Analysis and Risk Assessment for Automotive Security," *Information*, vol. 16, no. 6, p. 449, May 2025, doi: 10.3390/info16060449.

[35] G. Gori, L. Rinieri, A. Al Sadi, A. Melis, F. Callegati, and M. Prandini, "GRAPH4: A Security Monitoring Architecture Based on Data Plane Anomaly Detection Metrics Calculated over Attack Graphs," *Future Internet*, vol. 15, no. 11, p. 368, Nov. 2023, doi: 10.3390/fi15110368.

[36] A. Ahmad, A. Kovalenko, and I. Makarov, "Anomaly Detection Using Graph-Based Autoencoder with Graph Structure Learning Layer," in *2024 IEEE 6th International Symposium on Logistics and Industrial Informatics (LINDI)*, IEEE, Oct. 2024, pp. 89–94. doi: 10.1109/LINDI63813.2024.10820392.

[37] S. Rajasoundaran, S. A. Sivakumar, S. Devaraju, M. J. Pasha, and J. Lloret, "A deep experimental analysis of energy-proficient firewall policies and security practices for resource limited wireless networks," *SECURITY AND PRIVACY*, vol. 7, no. 6, Nov. 2024, doi: 10.1002/spy2.450.

[38] V. Govindarajan and J. H. Muzamal, "Advanced cloud intrusion detection framework using graph based features transformers and contrastive learning," *Sci. Rep.*, vol. 15, no. 1, p. 20511, Jul. 2025, doi: 10.1038/s41598-025-07956-w.

[39] A. V. Jha, B. Appasani, N. Bizon, and P. Thounthong, "A Graph-Theoretic Approach for Modelling and Resiliency Analysis of Synchrophasor Communication Networks," *Applied System Innovation*, vol. 6, no. 1, p. 7, Jan. 2023, doi: 10.3390/asi6010007.

[40] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," *IEEE Trans. Emerg. Top. Comput. Intell.*, vol. 2, no. 1, pp. 41–50, Feb. 2020, doi: 10.1109/TETCI.2017.2772792.

[41] A. S. Ahanger, S. M. Khan, F. Masoodi, and A. O. Salau, "Advanced intrusion detection in internet of things using graph attention networks," *Sci. Rep.*, vol. 15, no. 1, p. 9831, Mar. 2025, doi: 10.1038/s41598-025-94624-8.

[42] A. Lima, "Graph-Based Intrusion Detection for Edge-Cloud IoT Energy Systems," *Premier Journal of Computer Science*, Jan. 2026, doi: 10.70389/PJCS.100013.

[43] W. Jiang *et al.*, "Graph Neural Networks for Routing Optimization: Challenges and Opportunities," *Sustainability*, vol. 16, no. 21, p. 9239, Oct. 2024, doi: 10.3390/su16219239.

[44] C. Guerrero, I. Lera, and C. Juiz, "Genetic-based optimization in fog computing: Current trends and research opportunities," *Swarm Evol. Comput.*, vol. 72, no. 2, p. 101094, Jul. 2023, doi: 10.1016/j.swevo.2022.101094.

[45] L. Belcastro, C. Carlucci, C. Cosentino, P. Liò, and F. Marozzo, "Enhancing network security using knowledge graphs and large language models for explainable threat detection," *Future Generation Computer Systems*, vol. 176, no. 1, p. 108160, Mar. 2026, doi: 10.1016/j.future.2025.108160.

[46] M. Jaber, N. Boutry, and P. Parrend, "Graph-Based Spectral Analysis for Detecting Cyber Attacks," in *Proceedings of the 19th International Conference on Availability, Reliability and Security*, New York, NY, USA: ACM, Jul. 2024, pp. 1–14. doi: 10.1145/3664476.3664498.

[47] T. P. Doremure Gamage, J. A. Gutierrez, and S. K. Ray, "The Role of Graph Neural Networks, Transformers, and Reinforcement Learning in Network Threat Detection: A Systematic Literature Review," *Electronics (Basel).*, vol. 14, no. 21, p. 4163, Oct. 2025, doi: 10.3390/electronics14214163.