https://jurnal.pustakagalerimandiri.co.id/index.php/robotsister
DOI : https://doi.org/10.55382/jurnalpustakarobotsister.v4i2.2253

Jurnal Pustaka Robot Sister
Jurnal Pusat Akses Kajian Robotika, Sistem Tertanam, dan Sistem Terdistribusi
Vol. 4 No. 2 (2026) 113 – 121
E ISSN: 2987-1522

Systematic Literature Review: Artificial Intelligence untuk Klasifikasi pada Sistem Manajemen Jaringan Berbasis Web

Muhammad Rifqi Fadhlan Rahmatullah[1], Hana Kurnia Putri[2], Candhy Fadhila Arsyad[3]
Informatika, Fakultas Teknik, Universitas Doktor Nugroho Magetan
[1]mrifqi.fadhlanr.90@gmail.com, [2]hanaputri2818@gmail.com, [3]candhy.fadhila.arsyad@gmail.com

Abstract

This study aims to map the development of classification-based Artificial Intelligence (AI) in web-based network management systems and identify gaps between algorithmic advancement and operational implementation. A Systematic Literature Review was conducted using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) protocol. Relevant articles were retrieved from IEEE Xplore, MDPI, SpringerLink, ScienceDirect/Elsevier, Nature/Scientific Reports, Wiley Online Library, Frontiers, and selected national journals. Of 60 candidate articles published between 2021 and 2025, 50 met the inclusion, exclusion, and quality assessment criteria. The data were analyzed according to research themes, classification methods, dataset types, evaluation metrics, the role of web-based dashboards, and research gaps. The findings show that AI applications were dominated by network intrusion detection and classification at 40%, network management and traffic classification at 36%, and web attack classification at 24%. The methods evolved from classical Machine Learning toward Deep Learning, Ensemble Learning, Federated Learning, and hybrid models. However, integration with real-time dashboards, operational network data, interpretability, scalability, and usability evaluation remains limited. This study contributes an integrated research mapping, identifies implementation gaps, and proposes a framework for developing accurate, informative, adaptive, and user-friendly web-based network management systems to support rapid and appropriate decision-making by network administrators effectively.

Keywords: artificial intelligence, classification, network management, web-based system, systematic literature review

Abstrak

Penelitian ini bertujuan memetakan perkembangan penerapan *Artificial Intelligence* (*AI*) berbasis klasifikasi dalam sistem manajemen jaringan berbasis web serta mengidentifikasi kesenjangan antara pengembangan algoritma dan implementasinya pada sistem operasional. Penelitian menggunakan *metode Systematic Literature Review* dengan protokol *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (*PRISMA*). Artikel ditelusuri melalui *IEEE Xplore, MDPI, SpringerLink, ScienceDirect/Elsevier, Nature/Scientific Reports, Wiley Online Library, Frontiers*, dan jurnal nasional yang relevan. Dari 60 artikel kandidat yang diterbitkan pada periode 2021–2025, sebanyak 50 artikel memenuhi kriteria inklusi, eksklusi, dan penilaian kualitas. Data dianalisis berdasarkan tema penelitian, metode klasifikasi, jenis dataset, metrik evaluasi, peran web atau *dashboard*, serta kesenjangan penelitian. Hasil kajian menunjukkan bahwa penerapan *AI* didominasi oleh deteksi dan klasifikasi intrusi jaringan sebesar 40%, manajemen jaringan dan klasifikasi lalu lintas sebesar 36%, serta klasifikasi serangan web sebesar 24%. Metode yang digunakan berkembang dari *Machine Learning* klasik menuju *Deep Learning, Ensemble Learning, Federated Learning*, dan *Hybrid Model*. Namun, integrasi model dengan *dashboard real-time*, data jaringan operasional, interpretabilitas, skalabilitas, dan evaluasi kegunaan masih terbatas. Penelitian ini berkontribusi melalui pemetaan terpadu, identifikasi kesenjangan implementasi, serta usulan kerangka pengembangan sistem manajemen jaringan berbasis web yang akurat, informatif, adaptif, dan mudah digunakan untuk mendukung pengambilan keputusan administrator jaringan secara cepat dan tepat.

Submitted : 06-07-2026 | Reviewed : 09-07-2026 | Accepted : 18-07-2026

Kata kunci: kecerdasan buatan, klasifikasi, manajemen jaringan, sistem berbasis web, tinjauan literatur sistematis.

1. Pendahuluan

Jaringan komputer menjadi fondasi layanan digital, komputasi awan, *Internet of Things*, dan sistem terdistribusi. Pertumbuhan skala dan kompleksitas jaringan memunculkan kepadatan lalu lintas, gangguan konektivitas, anomali, serta serangan siber. Kajian terdahulu memperlihatkan bahwa klasifikasi berbasis *Machine Learning* dapat mendukung optimasi *QoS*, pengenalan trafik waktu nyata, klasifikasi pada *Software Defined Network*, perbandingan model deteksi intrusi, dan identifikasi serangan *SQL injection* [1]–[5].

Manajemen jaringan tidak cukup hanya menghasilkan model dengan akurasi tinggi. Administrator memerlukan informasi yang dapat ditindaklanjuti, seperti status trafik, indikasi gangguan, tingkat ancaman, dan rekomendasi respons. Karena itu, hasil klasifikasi perlu disajikan melalui *dashboard* web yang mendukung monitoring, visualisasi, pelaporan, dan pengambilan keputusan secara cepat.

Penelitian *intrusion detection* masih banyak menitikberatkan *class imbalance*, *anomaly detection*, *federated learning*, klasifikasi multikelas, serta pemetaan *dataset* dan tantangan model. Fokus tersebut penting untuk meningkatkan *detection rate* dan menekan *false alarm*, tetapi belum selalu diikuti pembahasan mengenai integrasi hasil ke sistem operasional [6]–[10],

Pada jaringan *IoT, SDN*, dan *Industrial Internet of Things, Deep Learning* dan *Hybrid Model* digunakan untuk mengenali pola serangan yang kompleks, menangani karakteristik spasial-temporal, serta menjaga privasi pemrosesan terdistribusi. Walaupun performanya menjanjikan, kebutuhan komputasi, ketersediaan data, dan kesiapan implementasi real-time tetap menjadi kendala [11]–[15].

Generalisasi lintas *dataset*, deteksi *SQL injection*, dan kajian keamanan aplikasi web menunjukkan bahwa performa tinggi pada dataset tertentu belum menjamin efektivitas pada lingkungan jaringan yang berbeda [16]–[18]. Kebaruan penelitian ini adalah pemetaan terpadu antara *AI* berbasis klasifikasi, manajemen jaringan, dan sistem berbasis web, mencakup metode, dataset, metrik, *dashboard*, dan gap implementasi.

Penelitian ini bertujuan mengidentifikasi tema dominan, metode klasifikasi, *dataset*, metrik evaluasi, peran web atau *dashboard*, serta peluang pengembangan sistem manajemen jaringan berbasis *AI*. Hasilnya diharapkan menjadi dasar teoretis dan praktis bagi sistem monitoring yang akurat, informatif, *real-time*, dan mudah digunakan.

2. Metode Penelitian

Penelitian menggunakan *Systematic Literature Review* dengan protokol *PRISMA* yang mencakup perumusan *research question*, pencarian artikel, penghapusan duplikasi, *screening, eligibility, quality assessment*, ekstraksi data, dan sintesis hasil. Dari 60 artikel kandidat tahun 2021–2025, sebanyak 50 artikel memenuhi kriteria dan dianalisis.

2.1. Research Question

Research Question menjadi pedoman pencarian, seleksi, ekstraksi, dan sintesis artikel sesuai ruang lingkup *AI*, klasifikasi, manajemen jaringan, dan sistem berbasis web, seperti yang tampak pada tabel 1.

Tabel 1. *Research Question*

No	Kode	***Research Question***
1	RQ1	Bagaimana penerapan *Artificial Intelligence* berbasis klasifikasi dalam manajemen jaringan berbasis web?
2	RQ2	Metode klasifikasi apa saja yang banyak digunakan dalam penelitian manajemen jaringan dan keamanan web?
3	RQ3	Objek jaringan apa saja yang banyak dikaji dalam penelitian terdahulu?
4	RQ4	Bagaimana peran web atau *dashboard* dalam mendukung manajemen jaringan berbasis *Artificial Intelligence*?
5	RQ5	Apa saja celah penelitian yang dapat dikembangkan dari kajian literatur terdahulu?

2.2. Sumber Data dan Strategi Pencarian

Artikel diperoleh dari *IEEE Xplore, MDPI, SpringerLink, ScienceDirect/ Elsevier, Nature/ Scientific Reports, Wiley Online Library, Frontiers*, serta jurnal nasional. *Publish or Perish* digunakan untuk penelusuran *metadata*, *Mendeley* untuk pengelolaan referensi dan pemeriksaan duplikasi, *Microsoft Excel* untuk ekstraksi dan tabulasi, sedangkan *VOSviewer* digunakan untuk visualisasi hubungan kata kunci, seperti yang bisa dilihat pada tabel 2.

Tabel 2. Distribusi Artikel Berdasarkan Database dan Penerbit

Database/Penerbit	Artikel Kandidat	Artikel Final
IEEE Xplore/IEEE Access	12	10
MDPI	20	18
SpringerLink/SpringerOpen	8	6
ScienceDirect/Elsevier	3	2
Nature/Scientific Reports	9	8
Wiley Online Library	2	1

Submitted : 06-07-2026 | Reviewed : 09-07-2026 | Accepted : 18-07-2026

Frontiers	2	1
Jurnal nasional dan sumber lain	4	4
Total	60	50

Distribusi sumber menunjukkan bahwa *MDPI, IEEE,* dan *Scientific Reports* memberikan kontribusi terbesar. Penggunaan beberapa database membantu memperluas cakupan literatur serta mengurangi ketergantungan pada satu penerbit.

Pencarian menggunakan kombinasi kata kunci terkait *network management, traffic classification, intrusion detection, anomaly detection, web security, Artificial Intelligence,* dan *Machine Learning* dengan *operator Boolean,* seperti yang dapat dilihat pada tabel 3.

Tabel 3. Strategi Pencarian Artikel

No	String Pencarian
1	"*network management*" AND "*artificial intelligence*" AND "*classification*"
2	"*network monitoring*" AND "*machine learning*" AND "*web-based system*"
3	"*network traffic classification*" AND "*machine learning*"
4	"*intrusion detection*" AND "*classification*" AND "*network security*"
5	"*website security*" AND "*machine learning*" AND "*classification*"
6	"*anomaly detection*" AND "*network traffic*" AND "*classification*"
7	"*web attack detection*" AND "*artificial intelligence*" AND "*classification*"
8	"*dashboard*" AND "*network monitoring*" AND "*machine learning*"

2.3. Kriteria Inklusi dan Eksklusi

Kriteria inklusi dan eksklusi diterapkan untuk menjaga relevansi, konsistensi, dan kelayakan metodologis artikel yang dianalisis, seperti tampak pada tabel 4 dan tabel 5.

Tabel 4. Kriteria Inklusi

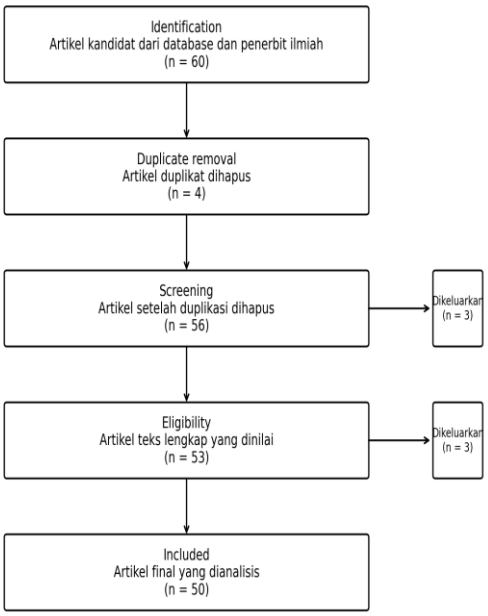
Kode	Kriteria Inklusi
IC1	Artikel diterbitkan pada rentang tahun 2021 sampai 2025.
IC2	Artikel membahas manajemen jaringan, monitoring jaringan, klasifikasi traffic jaringan, deteksi intrusi, deteksi anomali, atau keamanan website.
IC3	Artikel menggunakan *Artificial Intelligence*, Machine Learning, atau metode klasifikasi.
IC4	Artikel berasal dari jurnal, prosiding, atau sumber ilmiah yang relevan.
IC5	Artikel tersedia dalam bentuk *full text*.
IC6	Artikel menggunakan bahasa Indonesia atau bahasa Inggris.
IC7	Artikel memiliki informasi yang dapat diekstraksi, seperti metode, *dataset*, metrik evaluasi, hasil, atau gap penelitian.

Tabel 5. Kriteria Eksklusi

Kode	Kriteria Eksklusi
EC1	Artikel diterbitkan di luar rentang tahun 2021 sampai 2025.
EC2	Artikel tidak membahas jaringan komputer, keamanan jaringan, atau website.
EC3	Artikel tidak menggunakan pendekatan *Artificial Intelligence, Machine Learning*, atau klasifikasi.
EC4	Artikel hanya membahas *website* secara umum tanpa hubungan dengan jaringan atau keamanan.
EC5	Artikel hanya membahas *Artificial Intelligence* secara umum tanpa hubungan dengan manajemen jaringan.
EC6	Artikel berupa blog, artikel populer, opini, atau sumber nonilmiah.
EC7	Artikel duplikat atau memiliki pembahasan yang terlalu mirip dengan artikel lain.
EC8	Artikel tidak dapat diakses secara penuh atau tidak memiliki informasi metodologis yang memadai.

2.4. Seleksi Artikel dan *Quality Assessment*

Dari 60 artikel yang diidentifikasi, empat artikel duplikat dihapus. *Screening* terhadap 56 artikel mengeluarkan tiga artikel berdasarkan judul dan abstrak. Pemeriksaan teks lengkap terhadap 53 artikel kembali mengeluarkan tiga artikel, sehingga 50 artikel memenuhi kriteria akhir dan dianalisis. Alur tersebut dirangkum melalui diagram *PRISMA* dan tabel seleksi seperti pada gambar 1 dan tabel 6..



Gambar 1. *PRISMA Flow* Diagram Proses Seleksi Artikel

Tabel 6. Ringkasan Alur Seleksi *PRISMA*

Tahap *PRISMA*	Keterangan	Jumlah
Identification	Artikel kandidat dari database dan penerbit ilmiah	60
Duplicate removal	Artikel duplikat yang dihapus	4
Screening	Artikel setelah duplikasi dihapus	56
Screening	Artikel dikeluarkan berdasarkan judul dan abstrak	3
Eligibility	Artikel teks lengkap yang dinilai	53
Eligibility	Artikel dikeluarkan setelah pemeriksaan teks lengkap	3
Inclusion	Artikel final yang dianalisis	50

Quality assessment menilai kesesuaian topik, kejelasan metode, *dataset*, metrik evaluasi, serta kontribusi atau gap. Setiap indikator diberi skor 0,

0,5, atau 1; artikel dengan skor minimal 3 dipertahankan, seperti penyajian pada tabel 7.

Tabel 7. Indikator *Quality Assessment*

Kode	Pertanyaan *Quality Assessment*	Skor
QA1	Apakah artikel membahas *Artificial Intelligence, Machine Learning, Deep Learning*, atau metode klasifikasi?	0/0,5/1
QA2	Apakah artikel relevan dengan manajemen jaringan, klasifikasi lalu lintas, deteksi intrusi, deteksi anomali, atau keamanan web?	0/0,5/1
QA3	Apakah artikel menjelaskan metode atau algoritma klasifikasi secara jelas?	0/0,5/1
QA4	Apakah artikel menyebutkan dataset atau sumber data yang digunakan?	0/0,5/1
QA5	Apakah artikel menyajikan metrik evaluasi, hasil utama, keterbatasan, atau gap penelitian?	0/0,5/1

Tabel 8. Kategori Penilaian *Quality Assessment*

Rentang Skor	Kategori	Keputusan
4,00 sampai 5,00	Tinggi	Artikel dipertahankan
3,00 sampai 3,99	Sedang	Artikel dipertahankan
Di bawah 3,00	Rendah	Artikel dikeluarkan

Pada tabel 8, artikel dengan skor 4,00–5,00 dikategorikan tinggi, skor 3,00–3,99 dikategorikan sedang, sedangkan skor di bawah 3,00 dikeluarkan. Ambang ini memastikan bahwa artikel final menyediakan informasi metodologis yang memadai.

2.5. Ekstraksi dan Sintesis Data

Ekstraksi data mencakup penulis dan tahun, judul, sumber publikasi, fokus penelitian, objek jaringan, metode klasifikasi, *dataset*, metrik evaluasi, hasil utama, gap penelitian, dan peran web atau *dashboard*. Data disintesis secara deskriptif untuk karakteristik publikasi, secara tematik untuk pengelompokan fokus, secara komparatif untuk metode dan hasil, serta secara visual untuk menunjukkan pola hubungan antartopik, seperti pada tabel 9.

Tabel 9. Komponen Ekstraksi Data

No	Komponen Ekstraksi	Keterangan
1	Penulis dan tahun	Nama penulis dan tahun publikasi artikel.
2	Judul artikel	Judul artikel yang dianalisis.
3	*Database* atau sumber publikasi	Nama *database*, jurnal, prosiding, atau penerbit artikel.
4	Fokus penelitian	Topik utama artikel, seperti *intrusion detection, traffic classification, anomaly detection,* atau *web security*.
5	Objek jaringan	Objek yang dikaji, seperti lalu lintas jaringan, serangan jaringan, data *server*, *SDN*, *IoT*, atau keamanan web.
6	Metode klasifikasi	Metode *Artificial Intelligence, Machine Learning,* atau *Deep Learning* yang digunakan.
7	*Dataset*	*Dataset* atau sumber data yang digunakan dalam penelitian.
8	Metrik evaluasi	Ukuran evaluasi, seperti *accuracy, precision, recall, F1-score, detection rate, false alarm rate*, atau waktu komputasi.
9	Hasil utama	Temuan utama dari artikel.
10	Gap penelitian	Keterbatasan atau peluang pengembangan yang ditemukan dari artikel.
11	Peran web atau *dashboard*	Fungsi web sebagai media monitoring, visualisasi, pelaporan, atau objek keamanan.

3. Hasil dan Pembahasan

Hasil kajian disajikan berdasarkan karakteristik publikasi, tema penelitian, metode *AI*, *dataset*, metrik evaluasi, visualisasi kata kunci, tren, peran sistem web, dan gap penelitian.

3.1. Karakteristik Artikel

Publikasi meningkat tajam pada 2024–2025. Dari 50 artikel, 3 diterbitkan pada 2021, 1 pada 2022, 2 pada 2023, 16 pada 2024, dan 28 pada 2025; tahun 2025 menyumbang 56% artikel. Lengkapnya seperti pada tabel 10.

Tabel 10. Distribusi Artikel Berdasarkan Tahun Publikasi

Tahun	Jumlah Artikel	Persentase
2021	3	6%
2022	1	2%
2023	2	4%
2024	16	32%
2025	28	56%

Sumber publikasi didominasi *IEEE Access, Scientific Reports/Nature,* dan *jurnal MDPI*. Keragaman sumber menunjukkan bahwa klasifikasi jaringan bersifat *multidisipliner* dan berkaitan dengan keamanan siber, sistem informasi, *IoT, SDN*, serta aplikasi web, seperti tampak pada tabel 11.

Tabel 11. Distribusi Sumber Publikasi

Sumber Publikasi	Jumlah Artikel	Persentase
IEEE Access	10	20%
Scientific Reports/Nature	8	16%
Electronics/MDPI	9	18%
Applied Sciences/MDPI	5	10%
Computers/MDPI	2	4%
Future Internet/MDPI	2	4%
Jurnal dan sumber lainnya	14	28%

3.2. Klasifikasi Tema Penelitian

Artikel dikelompokkan menjadi *network intrusion detection/classification*, manajemen jaringan atau *traffic classification,* dan *website/web-attack classification* berdasarkan fokus dominannya, seperti tabel 12.

Tabel 12. Klasifikasi Tema Penelitian

Tema Penelitian	Jumlah Artikel	Persentase
Network intrusion detection/classification	20	40%
Manajemen jaringan/*traffic classification*	18	36%
Website/web attack classification	12	24%
Total	50	100%

Network intrusion detection/classification menjadi tema dominan dengan 20 artikel (40%). Kajian pada kelompok ini meliputi *Hybrid Model*, *feature selection, Deep Learning, information bottleneck,* dan *Federated Learning* untuk membedakan aktivitas normal, anomali, serta berbagai kelas serangan jaringan [19]–[23].

Traffic classification mencakup 18 artikel (36%) dan berfokus pada *SDN, self-supervised learning*, lalu lintas aplikasi, serta trafik terenkripsi. Sementara itu, kelompok *web-attack classification* membahas *multilabel web application firewall*, *autoencoder* untuk *SQL injection*, dan deteksi *command injection* [24]–[28].

Studi keamanan web juga menunjukkan perkembangan metode *Deep Learning* untuk mendeteksi *XSS* dan *SQL injection*, serta penggunaan model *Machine Learning* khusus untuk membedakan *payload* berbahaya dan normal [29], [30]. Meskipun demikian, hubungan keluaran model dengan *dashboard* manajemen jaringan masih terbatas.

3.3. Metode *Artificial Intelligence* yang Digunakan

Metode klasifikasi yang digunakan meliputi *Decision Tree, Random Forest, SVM, KNN, Naive Bayes, XGBoost, Neural Network, CNN, LSTM, Autoencoder, Transformer,* serta *deep graph convolutional network*. Studi-studi tersebut memperlihatkan variasi penerapan pada *SDN, trafik terenkripsi, web-attack detection,* dan *few-shot traffic classification* [31]–[35].

Tabel 13. Distribusi Kelompok Metode *AI*

Kelompok Metode	Jumlah Artikel	Persentase
Machine Learning klasik	12	24%
Ensemble Learning	8	16%
Deep Learning	15	30%
Feature-based Learning	5	10%
Federated Learning	3	6%
Hybrid Model	7	14%
Total	50	100%

Pada tabel 13, Deep Learning menjadi kelompok terbesar dengan 15 artikel (30%) karena mampu mengenali pola trafik dan serangan yang kompleks. Perkembangan terbaru mencakup zero-touch network security, intrusion detection untuk IoT, anomaly detection, multi-task learning pada label terbatas, serta encoder graf ringan untuk trafik terenkripsi [36]–[40].

Machine Learning klasik digunakan pada 12 artikel (24%) karena lebih sederhana, cepat dilatih, dan mudah diinterpretasikan. Pendekatan ini tetap relevan untuk dataset kecil hingga menengah, baseline eksperimen, dan lingkungan yang memiliki keterbatasan sumber daya komputasi.

Ensemble, Hybrid Model, dan *Federated Learning* digunakan untuk meningkatkan stabilitas, menangani *class imbalance*, menjaga privasi, serta mendeteksi serangan web yang kompleks. Penerapannya mencakup *resampling* dan optimasi fitur, *stacking*, *zero-day detection*, *CNN-BiLSTM-Attention,* dan *semantic embeddings* [41]–[45].

Metode lain yang berkembang meliputi *optimized extreme learning machine*, kajian *Deep Learning* untuk *network traffic classification, feature selection* pada *MQTT-IoT, 3D-CNN* untuk *dark-web traffic,* serta *supervised Machine Learning* pada jaringan *FiWi-IoT* [46]–[50]. Keragaman ini menunjukkan pergeseran dari model tunggal menuju pendekatan yang lebih adaptif dan kontekstual.

3.4 *Dataset* dan Metrik Evaluasi

Dataset dikelompokkan menjadi *network traffic, intrusion detection, SDN, IoT*, dan *web attack* sesuai fokus penelitian.

Tabel 14. Jenis *Dataset* yang Digunakan

Jenis *Dataset*	Jumlah Artikel	Persentase
Network traffic dataset	14	28%
Intrusion detection dataset	15	30%
SDN dataset	7	14%
IoT dataset	6	12%
Web attack dataset	8	16%
Total	50	100%

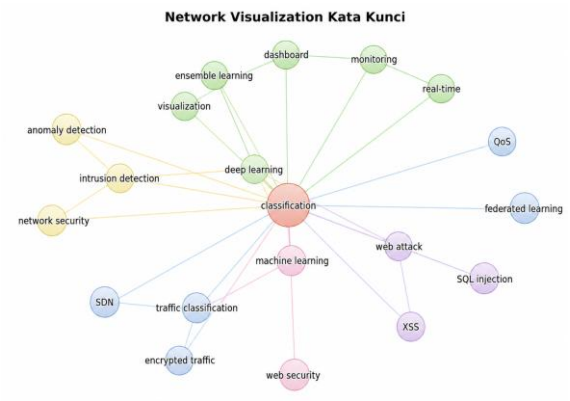
Intrusion detection dataset paling banyak digunakan, yaitu 15 artikel (30%), diikuti *network traffic dataset* sebanyak 14 artikel (28%). *SDN, IoT, dan web-attack dataset* digunakan sesuai kebutuhan domain. *Dataset* publik memudahkan replikasi dan perbandingan, tetapi karakteristiknya belum selalu merepresentasikan kondisi jaringan operasional, perubahan pola trafik, atau konfigurasi keamanan pada institusi tertentu.

Metrik utama meliputi *accuracy, precision, recall, F1-score, detection rate, false alarm rate,* dan *computational time*. Penggunaan *accuracy* saja kurang memadai pada data tidak seimbang, sehingga *precision, recall,* dan *F1-score* perlu dianalisis bersama. Evaluasi berikutnya juga perlu memasukkan *latency,* kebutuhan komputasi, interpretabilitas, kemampuan *real-time,* dan *usability dashboard*.

3.5 Visualisasi Kata Kunci

Network visualization dibuat menggunakan *VOSviewer* berdasarkan metadata judul, abstrak, dan kata kunci untuk melihat keterhubungan antartopik.

Visualisasi menghasilkan lima klaster, yaitu keamanan jaringan, *traffic classification*, keamanan aplikasi web, metode *AI*, serta *dashboard* dan *monitoring*. Istilah *machine learning, classification, intrusion detection,* dan *traffic classification* memiliki keterhubungan kuat, sedangkan *dashboard, real-time visualization,* dan *usability* muncul lebih terbatas. Pola ini memperkuat gap antara performa algoritma dan implementasi sistem. *Network visualization* kata kunci dapat dilihat pada gambar 2, dan interpretasi klaster kata kunci disajikan dalam tabel 15.



Gambar 2. *Network Visualization* Kata Kunci

Tabel 15. Interpretasi Klaster Kata Kunci

Klaster	Kata Kunci Dominan	Makna Klaster
Klaster 1	*intrusion detection, network security, anomaly detection, classification*	Fokus pada keamanan jaringan dan deteksi intrusi
Klaster 2	*traffic classification, SDN, QoS, encrypted traffic*	Fokus pada klasifikasi lalu lintas dan manajemen jaringan
Klaster 3	*web attack, SQL injection, XSS, web security*	Fokus pada keamanan aplikasi web
Klaster 4	*machine learning, deep learning, ensemble learning, federated learning*	Fokus pada pendekatan AI dan model klasifikasi
Klaster 5	*dashboard, monitoring, real-time, visualization*	Fokus pada sistem berbasis web dan visualisasi hasil

3.6 Tren Tema dan Metode Penelitian

Pada 2021–2023, penelitian terutama menggunakan *Machine Learning* dasar untuk *traffic classification* dan deteksi serangan web. Tahun 2024–2025 menunjukkan peningkatan tajam pada *intrusion detection, SDN, trafik terenkripsi, Deep Learning, Hybrid Model,* dan *Federated Learning*. Perkembangan tersebut belum diikuti secara seimbang oleh implementasi *dashboard*, evaluasi usability, dan pemantauan *real-time*, lengkapnya dapat dilihat pada tabel 16.

Tabel 16. Relasi Tema, Metode, dan Tahun Publikasi

Tahun	Tema Dominan	Metode Dominan	Jumlah Artikel
2021	*Traffic classification*	*Machine Learning* klasik	3
2022	*Web attack classification*	*Deep Learning*	1
2023	*Web attack classification*	*Autoencoder/ Deep Learning*	2
2024	*Intrusion detection* dan *traffic classification*	*Ensemble Learning* dan *Deep Learning*	16
2025	*Intrusion detection, traffic classification*, dan *web attack detection*	*Hybrid Model, Federated Learning,* dan *Deep Learning*	28

3.7 Peran Sistem Berbasis Web dan Gap Penelitian

Sistem berbasis web memiliki dua peran. Pertama, *dashboard* menyajikan kondisi jaringan, hasil klasifikasi, status anomali, tingkat ancaman, dan informasi pendukung keputusan. Kedua, aplikasi web menjadi objek keamanan yang perlu dilindungi dari *SQL injection, XSS, command injection, zero-day attack*, dan variasi *payload* berbahaya lainnya.

Sebagian besar penelitian masih berada pada tahap eksperimen algoritma. Integrasi model ke *dashboard real-time*, penggunaan data jaringan nyata, pengujian lintas *dataset*, interpretabilitas, dan evaluasi kebutuhan administrator belum memperoleh perhatian yang seimbang. Hal ini menimbulkan kesenjangan antara performa laboratorium dan pemanfaatan dalam pengelolaan jaringan sehari-hari.

Penelitian selanjutnya perlu mengembangkan *framework* yang menghubungkan akuisisi data jaringan, *preprocessing*, model klasifikasi, penyimpanan hasil, visualisasi *dashboard*, dan mekanisme peringatan. Evaluasi sebaiknya mencakup performa model, *latency*, skalabilitas, usability, interpretabilitas, serta kesesuaian informasi dengan tugas operasional administrator.

3.8 Sintesis Jawaban Research Question

RQ1 menunjukkan bahwa *AI* berbasis klasifikasi telah diterapkan pada tiga lapisan kebutuhan manajemen jaringan. Lapisan pertama adalah pengenalan kondisi lalu lintas, termasuk trafik aplikasi, trafik terenkripsi, dan komunikasi *IoT*. Lapisan kedua adalah perlindungan keamanan melalui deteksi intrusi, anomali, serta klasifikasi jenis serangan. Lapisan ketiga adalah penyajian informasi untuk mendukung keputusan administrator. Dua lapisan pertama telah banyak diuji melalui eksperimen algoritma, sedangkan lapisan penyajian dan pengambilan keputusan masih lebih jarang diwujudkan sebagai sistem operasional berbasis web.

RQ2 memperlihatkan bahwa tidak terdapat satu metode yang unggul untuk seluruh konteks. *Machine Learning* klasik sesuai untuk *baseline*, interpretasi, dan penggunaan sumber daya yang terbatas. *Deep Learning* lebih sesuai bagi pola trafik kompleks dan data berdimensi tinggi, tetapi membutuhkan data serta komputasi lebih besar. *Ensemble* dan *hybrid model* digunakan ketika stabilitas dan penanganan data tidak seimbang menjadi prioritas. *Federated Learning* menawarkan pemrosesan terdistribusi dan privasi, tetapi menambah kompleksitas komunikasi, sinkronisasi, dan pengelolaan model pada beberapa node.

RQ3 menghasilkan lima objek data utama, yaitu *network traffic, intrusion detection, SDN, IoT,* dan *web attack*. Perbedaan objek menentukan fitur,

skema pelabelan, jumlah kelas, serta metrik yang digunakan. *Dataset intrusion detection* dan *network traffic* paling dominan karena tersedia luas dan mudah dibandingkan. Namun, ketergantungan pada dataset publik dapat mengurangi kesesuaian model terhadap lingkungan organisasi yang memiliki topologi, kebijakan akses, jenis perangkat, serta pola penggunaan jaringan yang berbeda.

RQ4 menempatkan web dalam dua posisi yang saling melengkapi. Sebagai *dashboard*, web menjadi antarmuka untuk menampilkan status jaringan, hasil klasifikasi, tingkat ancaman, riwayat peristiwa, dan rekomendasi tindakan. Sebagai objek keamanan, aplikasi web perlu dilindungi dari *SQL injection, XSS, command injection*, dan serangan baru. Integrasi kedua posisi tersebut memungkinkan dashboard tidak hanya menampilkan kondisi jaringan, tetapi juga mengawasi keamanan aplikasi yang menjadi bagian dari layanan digital organisasi.

RQ5 menegaskan lima agenda penelitian. Pertama, model perlu diuji menggunakan data jaringan operasional dan skenario perubahan distribusi. Kedua, evaluasi harus melampaui *accuracy* dengan mempertimbangkan *F1-score, false alarm, latency*, kebutuhan komputasi, dan skalabilitas. Ketiga, hasil model perlu dijelaskan agar administrator memahami alasan suatu trafik diklasifikasikan sebagai ancaman. Keempat, *dashboard* harus diuji melalui usability dan kesesuaian informasi dengan tugas pengguna. Kelima, penelitian perlu menghubungkan eksperimen model, integrasi *API*, penyimpanan hasil, visualisasi, dan mekanisme peringatan dalam satu *framework* yang dapat dipelihara.

3.9 Rekomendasi Kerangka Pengembangan

Kerangka pengembangan yang disarankan terdiri atas akuisisi data jaringan, *preprocessing*, klasifikasi *AI*, layanan integrasi atau *API*, penyimpanan hasil, *dashboard*, dan mekanisme peringatan. Setiap komponen perlu dirancang modular agar model dapat diperbarui tanpa mengubah keseluruhan sistem. Rekomendasi perkembangan sistem ini dapat dilihat pada tabel 17.

Tabel 17. Rekomendasi Pengembangan Sistem

Aspek	Rekomendasi dan indikator evaluasi
Data	Trafik operasional anonim; cakupan kelas dan perubahan distribusi.
Model	*F1-score, false alarm, latency*, dan konsumsi sumber daya.
Integrasi	*API*, *logging* hasil, keandalan pertukaran data, dan waktu respons.
Dashboard	Status, ancaman, riwayat, penjelasan prediksi, dan uji *usability*.
Operasional	Pemantauan *real-time*, pembaruan model, dan prosedur respons insiden.

Kerangka tersebut perlu diuji pada skenario normal, lonjakan trafik, anomali, dan serangan. Evaluasi gabungan antara performa model dan pengalaman administrator akan menghasilkan sistem yang tidak hanya akurat, tetapi juga layak digunakan dalam operasi jaringan.

3.10 Keterbatasan Kajian

Kajian ini dibatasi pada artikel tahun 2021–2025 yang dapat diakses penuh dan ditemukan melalui database serta penerbit yang telah ditetapkan. Pembatasan tersebut menjaga kebaruan dan keterlacakan proses, tetapi masih memungkinkan adanya publikasi relevan yang tidak terjaring akibat perbedaan indeksasi, kata kunci, bahasa, atau akses dokumen. Distribusi artikel yang lebih banyak berasal dari beberapa penerbit juga dapat menimbulkan bias sumber.

Pengelompokan tema, metode, dan dataset dilakukan berdasarkan fokus dominan setiap artikel. Artikel yang menggunakan beberapa algoritma sekaligus tetap ditempatkan pada satu kelompok utama agar jumlah keseluruhan tidak dihitung ganda. Konsekuensinya, tabel distribusi menggambarkan kecenderungan literatur, bukan peringkat mutlak keberhasilan algoritma. Perbedaan dataset, skema validasi, jumlah kelas, dan kondisi eksperimen juga membatasi perbandingan langsung antarhasil penelitian.

Analisis peran *dashboard* dan sistem berbasis web disusun dari informasi implementasi yang tersedia pada artikel. Sebagian penelitian hanya menjelaskan model pada tingkat eksperimen sehingga aspek arsitektur, keamanan integrasi, pengalaman pengguna, dan pemeliharaan sistem tidak selalu dilaporkan secara lengkap. Karena itu, rekomendasi kerangka pengembangan perlu divalidasi melalui studi implementasi, pengujian dengan data jaringan nyata, serta evaluasi bersama administrator sebagai pengguna utama

3.11 Implikasi Teoretis dan Praktis

Secara teoretis, hasil kajian memperjelas bahwa keberhasilan klasifikasi jaringan perlu dipahami sebagai hubungan antara kualitas data, karakteristik metode, konteks objek, dan kebutuhan pengguna. Perbandingan algoritma tidak cukup dilakukan hanya melalui satu nilai accuracy, karena keputusan model dipengaruhi oleh ketidakseimbangan kelas, perubahan pola trafik, pemilihan fitur, dan skema validasi. Kerangka analisis yang menggabungkan performa, efisiensi, interpretabilitas, serta kesiapan integrasi dapat digunakan untuk menilai kontribusi penelitian secara lebih menyeluruh.

Secara metodologis, penelitian *SLR* berikutnya dapat memperkuat keterlacakan dengan menyediakan protokol pencarian, daftar artikel yang diseleksi, skor *quality assessment*, dan lembar ekstraksi sebagai lampiran. Analisis bibliometrik dapat dipadukan dengan sintesis isi sehingga keterhubungan kata kunci tidak hanya menunjukkan frekuensi, tetapi juga menjelaskan perbedaan tujuan, dataset, konfigurasi eksperimen, dan hasil.

Pembaruan kajian secara berkala juga diperlukan karena metode, dataset, dan pola serangan jaringan berubah dengan cepat.

Secara praktis, organisasi dapat menggunakan hasil pemetaan untuk menentukan prioritas pengembangan. Lingkungan dengan sumber daya terbatas dapat memulai dari model *Machine Learning* yang ringan dan mudah dijelaskan, sedangkan lingkungan dengan trafik kompleks dapat mempertimbangkan *Deep Learning* atau *Hybrid Model*. Pemilihan metode harus diikuti rancangan integrasi, tata kelola data, pembaruan model, keamanan *API*, pencatatan peristiwa, serta dashboard yang menampilkan informasi sesuai tingkat kewenangan pengguna. Dengan pendekatan tersebut, model *AI* tidak berhenti sebagai prototipe, tetapi menjadi bagian dari proses monitoring dan respons insiden.

4. Kesimpulan

Kajian terhadap 50 artikel tahun 2021–2025 menunjukkan bahwa *AI* berbasis klasifikasi paling banyak diterapkan pada *intrusion detection, traffic classification, anomaly detection, keamanan IoT, SDN,* dan *web-attack detection*. Metode berkembang dari *Machine Learning* klasik menuju *Deep Learning, Ensemble Learning, Federated Learning,* dan *Hybrid Model*. Meskipun performa algoritma terus meningkat, integrasi hasil ke *dashboard* berbasis web, penggunaan data jaringan nyata, evaluasi *real-time, usability*, dan interpretabilitas masih terbatas. Arah penelitian berikutnya adalah sistem manajemen jaringan berbasis web yang menggabungkan klasifikasi *AI*, visualisasi informatif, dan kebutuhan operasional pengguna.

Daftar Rujukan

[1] R. H. Serag, M. S. Abdalzaher, H. A. E. A. Elsayed, and M. Sobh, "Software Defined Network Traffic Classification for QoS Optimization Using Machine Learning," *J. Netw. Syst. Manag.*, vol. 33, no. 2, Apr. 2025, doi: 10.1007/s10922-025-09911-6.

[2] A. A. Ahmed and G. Agunsoye, "A real-time network traffic classifier for online applications using machine learning," *Algorithms*, vol. 14, no. 8, Aug. 2021, doi: 10.3390/a14080250.

[3] R. H. Serag, M. S. Abdalzaher, H. A. E. A. Elsayed, M. Sobh, M. Krichen, and M. M. Salim, "Machine-Learning-Based Traffic Classification in Software-Defined Networks," *Electronics (Switzerland)*, vol. 13, no. 6. Multidisciplinary Digital Publishing Institute (MDPI), Mar. 01, 2024. doi: 10.3390/electronics13061108.

[4] M. L. Ali, K. Thakur, S. Schmeelk, J. Debello, and D. Dragos, "Deep Learning vs. Machine Learning for Intrusion Detection in Computer Networks: A Comparative Study," *Appl. Sci.*, vol. 15, no. 4, Feb. 2025, doi: 10.3390/app15041903.

[5] Z. Gui *et al.*, "SqliGPT: Evaluating and Utilizing Large Language Models for Automated SQL Injection Black-Box Detection," *Appl. Sci.*, vol. 14, no. 16, 2024, doi: 10.3390/app14166929.

[6] V. Shanmugam, R. Razavi-Far, and E. Hallaji, "Addressing Class Imbalance in Intrusion Detection: A Comprehensive Evaluation of Machine Learning Approaches," *Electron.*, vol. 14, no. 1, Jan. 2025, doi: 10.3390/electronics14010069.

[7] H. Park, D. Shin, C. Park, J. Jang, and D. Shin, "Unsupervised Machine Learning Methods for Anomaly Detection in Network Packets," *Electron.*, vol. 14, no. 14, pp. 1–14, 2025, doi: 10.3390/electronics14142779.

[8] M. Devine, S. P. Ardakani, M. Al-Khafajiy, and Y. James, "Federated Machine Learning to Enable Intrusion Detection Systems in IoT Networks," *Electron.*, vol. 14, no. 6, 2025, doi: 10.3390/electronics14061176.

[9] F. A. Khan *et al.*, "Balanced Multi-Class Network Intrusion Detection Using Machine Learning," *IEEE Access*, vol. 12, pp. 178222–178236, 2024, doi: 10.1109/ACCESS.2024.3503497.

[10] H. M. R. U. Rehman *et al.*, "A systematic literature study of machine learning techniques based intrusion detection: datasets, models, challenges, and future directions," *J. Big Data*, vol. 12, no. 1, 2025, doi: 10.1186/s40537-025-01323-2.

[11] M. A. Hossain, "Deep learning-based intrusion detection for IoT networks: a scalable and efficient approach," *Eurasip J. Inf. Secur.*, vol. 2025, no. 1, 2025, doi: 10.1186/s13635-025-00202-w.

[12] J. Saikam and K. Ch, "EESNN: Hybrid Deep Learning Empowered Spatial-Temporal Features for Network Intrusion Detection System," *IEEE Access*, vol. 12, pp. 15930–15945, 2024, doi: 10.1109/ACCESS.2024.3350197.

[13] M. Raza, M. Jasim Saeed, M. B. Riaz, and M. Awais Sattar, "Federated Learning for Privacy-Preserving Intrusion Detection in Software-Defined Networks," *IEEE Access*, vol. 12, pp. 69551–69567, 2024, doi: 10.1109/ACCESS.2024.3395997.

[14] N. H. S. Al-Sarray, A. Demirhan, and J. Rahebi, "A robust and scalable intrusion detection framework for SDN with GAN-CL-STO," *J. Supercomput.*, vol. 81, no. 14, Sep. 2025, doi: 10.1007/s11227-025-07821-7.

[15] S. I. Popoola, Y. Tsado, A. A. Ogunjinmi, E. Sanchez-Velazquez, Y. Peng, and D. B. Rawat, "Multi-Stage Deep Learning for Intrusion Detection in Industrial Internet of Things," *IEEE Access*, vol. 13, pp. 60532–60555, 2025, doi: 10.1109/ACCESS.2025.3557959.

[16] M. Cantone, C. Marrocco, and A. Bria, "Machine Learning in Network Intrusion Detection: A Cross-Dataset Generalization Study," *IEEE Access*, vol. 12, pp. 144489–144508, 2024, doi: 10.1109/ACCESS.2024.3472907.

[17] E. Casmiry, N. Mduma, and R. Sinde, "Enhanced SQL injection detection using chi-square feature selection and machine learning classifiers," *Front. Big Data*, vol. 8, 2025, doi: 10.3389/fdata.2025.1686479.

[18] R. L. Alaoui and E. H. Nfaoui, "Deep Learning for Vulnerability and Attack Detection on Web Applications: A Systematic Literature Review," *Future Internet*, vol. 14, no. 4. MDPI, Apr. 01, 2022. doi: 10.3390/fi14040118.

[19] M. Sajid *et al.*, "Enhancing intrusion detection: a hybrid machine and deep learning approach," *J. Cloud Comput.*, vol. 13, no. 1, Dec. 2024, doi: 10.1186/s13677-024-00685-x.

[20] E. Emirmahmutoğlu and Y. Atay, "A feature selection-driven machine learning framework for anomaly-based intrusion detection systems," *Peer-to-Peer Netw. Appl.*, vol. 18, no. 3, Jun. 2025, doi: 10.1007/s12083-025-01947-4.

[21] M. Farhan *et al.*, "Network-based intrusion detection using deep learning technique," *Sci. Rep.*, vol. 15, no. 1, Dec. 2025, doi: 10.1038/s41598-025-08770-0.

[22] W. Lin and Y. Chen, "Robust Network Traffic Classification Based on Information Bottleneck Neural Network," *IEEE Access*, vol. 12, pp. 150169–150179, 2024, doi: 10.1109/ACCESS.2024.3477466.

[23] H. Xue, Y. Hu, and Y. Wang, "Federated Distributed Network Traffic Classification Based on Deep Mutual Learning," *Electron.*, vol. 14, no. 24, Dec. 2025, doi: 10.3390/electronics14244928.

[24] D. Nuñez-Agurto, W. Fuertes, L. Marrone, E. Benavides-Astudillo, C. Coronel-Guerrero, and F. Perez, "A Novel Traffic Classification Approach by Employing Deep Learning on Software-Defined Networking," *Futur. Internet*, vol. 16, no. 5, May 2024, doi: 10.3390/fi16050153.

[25] E. Eslami and W. Hamouda, "Network Traffic Classification Using Self-Supervised Learning and Confident Learning," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 9100–9120, 2025, doi: 10.1109/OJCOMS.2025.3625534.

[26] C. Chindrus and C. F. Caruntu, "Machine Learning-Based Multilabel Classification for Web Application Firewalls: A Comparative Study," *Electron.*, vol. 14, no. 21, Nov. 2025, doi: 10.3390/electronics14214172.

[27] N. Thalji, A. Raza, M. S. Islam, N. A. Samee, and M. M. Jamjoom, "AE-Net: Novel Autoencoder-Based Deep Features for SQL Injection Attack Detection," *IEEE Access*, vol. 11, pp. 135507–135516, 2023, doi: 10.1109/ACCESS.2023.3337645.

[28] X. Wang, J. Zhai, and H. Yang, "Detecting command injection attacks in web applications based on novel deep learning methods," *Sci. Rep.*, vol. 14, no. 1, Dec. 2024, doi: 10.1038/s41598-024-74350-3.

[29] J. R. Tadhani, V. Vekariya, V. Sorathiya, S. Alshathri, and W. El-Shafai, "Securing web applications against XSS and SQLi attacks using a novel deep learning approach," *Sci. Rep.*, vol. 14, no. 1, Dec. 2024, doi: 10.1038/s41598-023-48845-4.

[30] C. M. Rosca, A. Stancu, and C. Popescu, "Machine Learning Models for SQL Injection Detection," *Electron.*, vol. 14, no. 17, Sep. 2025, doi: 10.3390/electronics14173420.

[31] A. O. Salau and M. M. Beyene, "Software defined networking based network traffic classification using machine learning techniques," *Sci. Rep.*, vol. 14, no. 1, Dec. 2024, doi: 10.1038/s41598-024-70983-6.

[32] R. T. Elmaghraby, N. M. Abdel Aziem, M. A. Sobh, and A. M. Bahaa-Eldin, "Encrypted network traffic classification based on machine learning," *Ain Shams Eng. J.*, vol. 15, no. 2, p. 102361, 2024, doi: 10.1016/j.asej.2023.102361.

[33] Z. Liu, Y. Xie, Y. Luo, Y. Wang, and X. Ji, "TransECA-Net: A Transformer-Based Model for Encrypted Traffic Classification," *Appl. Sci.*, vol. 15, no. 6, 2025, doi: 10.3390/app15062977.

[34] A. Salam, F. Ullah, F. Amin, and A. Mohammad, "Deep Learning Techniques for Web-Based Attack Detection in," *Mdpi*, pp. 1–18, 2023.

[35] S. Xu, J. Han, Y. Liu, H. Liu, and Y. Bai, "Few-shot traffic classification based on autoencoder and deep graph convolutional networks," *Sci. Rep.*, vol. 15, no. 1, Dec. 2025, doi: 10.1038/s41598-025-94240-6.

[36] E. U. H. Qazi, T. Zia, M. Hamza Faheem, K. Shahzad, M. Imran, and Z. Ahmed, "Zero-Touch Network Security (ZTNS): A Network Intrusion Detection System Based on Deep Learning," *IEEE Access*, vol. 12, pp. 141625–141638, 2024, doi: 10.1109/ACCESS.2024.3466470.

[37] L. A. Maghrabi, "Automated Network Intrusion Detection for Internet of Things: Security Enhancements," *IEEE Access*, vol. 12, pp. 30839–30851, 2024, doi: 10.1109/ACCESS.2024.3369237.

[38] S. Ness, V. Eswarakrishnan, H. Sridharan, V. Shinde, N. Venkata Prasad Janapareddy, and V. Dhanawat, "Anomaly Detection in Network Traffic Using Advanced Machine Learning Techniques," *IEEE Access*, vol. 13, pp. 16133–16149, 2025, doi: 10.1109/ACCESS.2025.3526988.

[39] L. Liu, Y. Yu, Y. Wu, Z. Hui, J. Lin, and J. Hu, "Method for multi-task learning fusion network traffic classification to address small sample labels," *Sci. Rep.*, vol. 14, no. 1, Dec. 2024, doi: 10.1038/s41598-024-51933-8.

[40] Z. W. Chen, X. X. Wei, and Y. S. Wang, "Encrypted traffic classification encoder based on lightweight graph representation," *Sci. Rep.*, vol. 15, no. 1, pp. 1–14, 2025, doi: 10.1038/s41598-025-05225-4.

[41] N. Nigar and R. Mustafa, "Enhanced Intrusion Detection via Hybrid Data Resampling and Feature Optimization," *IEEE Access*, vol. 13, pp. 149100–149120, 2025, doi: 10.1109/ACCESS.2025.3602562.

[42] M. A. Talukder *et al.*, "Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction," *J. Big Data*, vol. 11, no. 1, Dec. 2024, doi: 10.1186/s40537-024-00886-w.

[43] V. Babaey and H. R. Faragardi, "Detecting Zero-Day Web Attacks with an Ensemble of LSTM, GRU, and Stacked Autoencoders," *Computers*, vol. 14, no. 6, Jun. 2025, doi: 10.3390/computers14060205.

[44] Z. Li, F. Liu, Z. Gu, and Y. Liu, "XSS Attack Detection Method Based on CNN-BiLSTM-Attention," *Appl. Sci.*, vol. 15, no. 16, Aug. 2025, doi: 10.3390/app15168924.

[45] R. Bakır and H. Bakır, "Swift Detection of XSS Attacks: Enhancing XSS Attack Detection by Leveraging Hybrid Semantic Embeddings and AI Techniques," *Arab. J. Sci. Eng.*, vol. 50, no. 2, pp. 1191–1207, Jan. 2025, doi: 10.1007/s13369-024-09140-0.

[46] X. Zhang and J. Yin, "Optimized extreme learning machines with deep learning for high-performance network traffic classification," *Sci. Rep.*, vol. 15, no. 1, Dec. 2025, doi: 10.1038/s41598-025-16980-9.

[47] N. Bayat, W. Jackson, and D. Liu, "Deep Learning for Network Traffic Classification," Jun. 2021, [Online]. Available: http://arxiv.org/abs/2106.12693

[48] E. Tuyishime, M. Martalò, P. A. Cotfas, V. Popescu, D. T. Cotfas, and A. Rekeraho, "Resource-Efficient Traffic Classification Using Feature Selection for Message Queuing Telemetry Transport-Internet of Things Network-Based Security Attacks," *Appl. Sci.*, vol. 15, no. 8, Apr. 2025, doi: 10.3390/app15084252.

[49] J. Li, Z. Pan, and K. Jiang, "A Three-Dimensional Convolutional Neural Network for Dark Web Traffic Classification Based on Multi-Channel Image Deep Learning," *Computers*, vol. 14, no. 8, Aug. 2025, doi: 10.3390/computers14080295.

[50] E. Ganesan, I.-S. Hwang, A. T. Liem, M. Syuhaimi, and A.- Rahman, "photonics hv SDN-Enabled FiWi-IoT Smart Environment Network Traffic Classification Using Supervised ML Models," 2021, doi: 10.3390/photonics.