JURNAL RISET INFORMATIKA **P-ISSN: 2656-1743 |E-ISSN: 2656-1735**
Vol. 8, No. 4. September 2026 DOI: https://doi.org/10.34288/jri.v8i4.552
Accredited rank 4 (SINTA 4), excerpts from the decision of the DITJEN DIKTIRISTEK No. 230/E/KPT/2023

DEEP LEARNING-BASED INTRUSION DETECTION SYSTEMS: ARCHITECTURES, IMPLEMENTATIONS, AND CHALLENGES IN MODERN NETWORK ANOMALY DETECTION

Ahmad Zulham Fahamsyah Havy[-1*], Muhammad Faishol Amrulloh[-2]

Teknik Informatika
Universitas Yudharta Pasuruan
zulham92@yudharta.ac.id[-1*], faishol@yudharta.ac.id[-2]

Abstract

The increasing complexity of cyber threats has strengthened the need for adaptive network intrusion detection systems (IDS). This systematic literature review (SLR) synthesizes nine peer-reviewed studies published from 2024 to 2026 on deep learning (DL)-based network anomaly detection. The review follows a PRISMA 2020-aligned process covering database selection, eligibility screening, quality assessment, and structured data extraction. Five research questions examine DL architectures, preprocessing and class-imbalance handling, comparative performance, deployment challenges, and the basis for a conceptual framework. The synthesis compares preprocessing, classification strategy, Accuracy, Precision, Recall, and F1-Score where reported. The evidence shows that hybrid architectures can achieve very high benchmark performance, but the results are dataset- and experimental-setting dependent; therefore, the claim that hybrid models universally exceed 95% is not supported. Across the included studies, the recurring technical pattern is: representative data collection, preprocessing and imbalance mitigation, architecture selection according to spatial or temporal characteristics, and multi-metric evaluation. The revised framework extends this four-layer pipeline by explicitly integrating Explainable AI (XAI) and edge-oriented deployment as cross-cutting operational requirements. The review also identifies limitations in dataset realism, cross-dataset validation, reporting consistency, computational efficiency, and explainability.

Keywords: Deep Learning; Anomaly Detection; Cyber Security; Intrusion Detection System; Hybrid Model; Systematic Literature Review

Abstrak

*Meningkatnya kompleksitas ancaman siber telah memperkuat kebutuhan akan sistem deteksi intrusi jaringan (IDS) yang adaptif. Tinjauan pustaka sistematis (SLR) ini menyintesis sembilan studi yang telah melalui penelaahan sejawat (peer-reviewed) dan diterbitkan antara tahun 2024 hingga 2026 mengenai deteksi anomali jaringan berbasis *deep learning* (DL). Tinjauan ini mengikuti proses yang selaras dengan pedoman PRISMA 2020, yang mencakup pemilihan basis data, penyaringan kelayakan, penilaian kualitas, dan ekstraksi data secara terstruktur. Lima pertanyaan penelitian mengkaji arsitektur DL, pra-pemrosesan dan penanganan ketidakseimbangan kelas, perbandingan kinerja, tantangan penerapan, serta dasar bagi kerangka kerja konseptual. Sintesis ini membandingkan pra-pemrosesan, strategi klasifikasi, serta metrik Akurasi, Presisi, *Recall*, dan *F1-Score* pada studi-studi yang melaporkannya. Bukti menunjukkan bahwa arsitektur hibrida mampu mencapai kinerja tolok ukur yang sangat tinggi, namun hasilnya bergantung pada kumpulan data dan pengaturan eksperimen; oleh karena itu, klaim bahwa model hibrida secara universal melampaui tingkat akurasi 95% tidak terbukti. Pola teknis yang berulang dalam studi-studi tersebut meliputi: pengumpulan data yang representatif, pra-pemrosesan dan mitigasi ketidakseimbangan data, pemilihan arsitektur berdasarkan karakteristik spasial atau temporal, serta evaluasi menggunakan berbagai metrik. Kerangka kerja yang telah direvisi memperluas alur kerja empat tahap ini dengan secara eksplisit mengintegrasikan *Explainable AI* (XAI) dan penerapan berbasis *edge* sebagai persyaratan operasional lintas aspek. Tinjauan ini juga mengidentifikasi keterbatasan terkait realisme kumpulan data, validasi lintas kumpulan data, konsistensi pelaporan, efisiensi komputasi, dan kemampuan untuk dijelaskan.*

Kata kunci: Deep Learning; Deteksi Anomali; Keamanan Siber; Sistem Deteksi Intrusi; Model Hibrida; Tinjauan Pustaka Sistematis

INTRODUCTION

Networked systems have become increasingly heterogeneous, connecting cloud services, software-defined networks (SDN), Internet of Things (IoT) devices, and critical infrastructure. This expansion also increases the diversity and dynamism of attack behavior. Recent reviews emphasize that deep learning (DL) is increasingly used in network-based intrusion detection because it can learn nonlinear and sequential representations from traffic without relying entirely on manually engineered rules (Ali et al., 2024; Wu et al., 2024; Anis et al., 2025).

However, high benchmark performance does not automatically imply operational effectiveness. Class imbalance can cause a model to favor majority traffic, while a model that performs well on one benchmark may degrade on another. Recent studies also show that preprocessing, feature selection, model architecture, and dataset characteristics can materially change performance (Odeh & Taleb, 2024; Ataa et al., 2024; Düzgün et al., 2024).

Hybrid models are particularly prominent because CNNs can capture local feature relationships while recurrent or attention-based components can model temporal or contextual dependencies. For example, Ataa et al. (2024) reported 99.19% accuracy for a CNN-LSTM configuration on the InSDN dataset, while Alharthi (2024) reported 99.99% for ConvLSTM on selected benchmark settings. Kamal and Mashaly (2025) also reported accuracy above 99.9% for several binary and multi-class configurations. These results are strong, but they arise from specific datasets and experimental protocols and therefore should not be generalized as a universal property of hybrid models.

The literature also exposes a methodological gap. Existing surveys provide broad taxonomies of architectures and datasets, while some recent studies focus on particular environments such as SDN, IoT, or government data centers (Chinnasamy et al., 2025; Anis et al., 2025; Rotib et al., 2026). What remains useful for an applied informatics audience is a recent, auditable synthesis that links preprocessing, classification architecture, reported metrics, class-imbalance handling, explainability, and deployment constraints in one framework.

Accordingly, the research gap addressed by this SLR is the limited integration of technical performance evidence with operational requirements in a single recent synthesis. The novelty of this review is therefore methodological and integrative rather than the proposal of a new predictive algorithm: it (1) restricts the core evidence set to recent peer-reviewed studies; (2) makes the selection and quality-assessment criteria explicit; (3) compares preprocessing, classification, and four standard performance metrics; and (4) derives a four-layer architecture with XAI and edge deployment treated as cross-cutting requirements.

Research Questions

1. RQ1. Which deep learning architectures and classification strategies are most frequently applied to network intrusion/anomaly detection in the recent literature?
2. RQ2. Which preprocessing, feature-engineering, and class-imbalance handling techniques are used before model training?
3. RQ3. What Accuracy, Precision, Recall, and F1-Score results are reported, and what evidence supports comparisons among model families?
4. RQ4. What operational challenges—particularly explainability, computational cost, latency, scalability, and deployment environment—limit practical adoption?
5. RQ5. How can the findings be synthesized into a conceptual framework that is traceable to the reviewed evidence?

RESEARCH METHODS

This study uses a Systematic Literature Review (SLR) design and follows the reporting principles of PRISMA 2020. PRISMA 2020 emphasizes transparent reporting of the search, selection, and synthesis process and provides a flow-diagram structure for systematic reviews (Page et al., 2021). The present review is designed as a structured qualitative and comparative synthesis rather than a meta-analysis because the included studies use heterogeneous datasets, model configurations, and evaluation protocols.

Search Strategy and Database Selection

The search strategy was designed to prioritize peer-reviewed literature indexed or hosted by reputable scientific publishers. The core databases/sources were IEEE Xplore, ScienceDirect, SpringerLink, MDPI, and DOAJ. arXiv was excluded from the core evidence set because it is a preprint repository rather than a peer-reviewed journal database. The search window was January 2024 to March 2026.

The principal search string was: ("deep learning" OR "deep neural network" OR CNN OR

LSTM OR Transformer OR "hybrid deep learning") AND ("intrusion detection" OR "network anomaly detection" OR NIDS) AND (network OR cybersecurity OR IoT OR SDN). Database-specific syntax was adapted where necessary while preserving the same conceptual terms.

Inclusion and Exclusion Criteria

Tabel 1. Inclusion and Exclusion Criteria for Literature Selection

Code	Criterion
IC1	Published between 2024 and March 2026.
IC2	Peer-reviewed journal or peer-reviewed scholarly publication with verifiable bibliographic metadata and DOI where available.
IC3	Focuses on network intrusion/anomaly detection using DL or a DL-hybrid architecture.
IC4	Reports a dataset, preprocessing/training procedure, model architecture, and at least one evaluation result.
IC5	Provides sufficient full-text information for structured extraction.
EC1	Preprints, duplicate records, unrelated cybersecurity topics, and studies outside network intrusion/anomaly detection.
EC2	Papers without enough methodological or performance information to support the review questions.

Screening and Study Selection

Screening was conducted in three stages: (1) title/abstract relevance, (2) full-text eligibility, and (3) methodological quality assessment. The original submission did not preserve the database export files or exact hit counts. To avoid inventing unverifiable numbers, this reports the auditable final evidence set of nine included peer-reviewed studies and documents the decision rules rather than reconstructing database-hit counts after the fact. The final set consists of studies by Sari et al. (2024), Yu et al. (2024), Odeh and Taleb (2024), Alharthi (2024), Ataa et al. (2024), Düzgün et al. (2024), Kamal and Mashaly (2025), Almuhanna and Dardouri (2025), and Rotib et al. (2026).

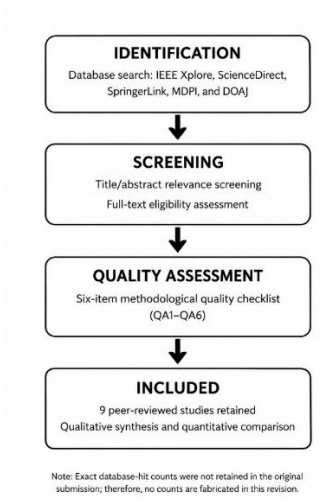

Figure 1. PRISMA 2020-aligned screening pathway used in the revised SLR.

Quality Assessment

Each included study was assessed using six binary questions: QA1: research objective is explicit; QA2: dataset is identified; QA3: preprocessing/feature preparation is described; QA4: model architecture/classification procedure is described; QA5: evaluation metrics are reported; QA6: validation/testing procedure is described. One point was assigned for each criterion satisfied. Studies scoring at least 4/6 were retained. The assessment is intended to judge reporting quality for synthesis, not to rank the scientific merit of the original authors.

Tabel 2. Quality Assessment Results of the Selected Primary Studies

Study	QA1	QA2	QA3	QA4	QA5	QA6	Score
Sari et al. (2024)	Yes	Yes	Yes	Yes	Yes	No	5/6
Yu et al. (2024)	Yes	Yes	Partial	Yes	Partial	Yes	5/6
Odeh & Taleb (2024)	Yes	Yes	Yes	Yes	Yes	Yes	6/6
Alharthi (2024)	Yes	Yes	Yes	Yes	Yes	Yes	6/6
Ataa et al. (2024)	Yes	Yes	Yes	Yes	Yes	Yes	6/6
Düzgün et al. (2024)	Yes	Yes	Yes	Yes	Yes	Yes	6/6
Kamal & Mashaly (2025)	Yes	Yes	Yes	Yes	Yes	Yes	6/6
Almuhanna & Dardouri (2025)	Yes	Yes	Yes	Yes	Yes	Yes	6/6
Rotib et al. (2026)	Yes	Yes	Yes	Yes	Yes	Yes	6/6

Data Extraction and Analysis

A standardized extraction form was used to record publication year, dataset, preprocessing, imbalance handling, architecture, classification type, Accuracy, Precision, Recall, F1-Score, validation approach, and deployment implications. Missing metrics are explicitly marked NR (not reported in the accessible study text) rather than estimated. The synthesis uses content analysis and functional comparison. Because datasets and

experimental protocols are heterogeneous, the reported metric values are compared descriptively and are not pooled statistically.

Evaluation Metrics and Model Components

The sigmoid activation function is a model component used, among other settings, for binary classification outputs; it is not an evaluation metric. It can be expressed as:

$$f(x) = 1 / (1 + e^{(-x)})$$

Model evaluation is separated from activation functions. Accuracy measures the proportion of correct predictions:

$$Accuracy = (TP + TN) / (TP + TN + FP + FN)$$

Precision, Recall, and F1-Score are reported where available. F1-Score summarizes the balance between Precisiown and Recall; it does not itself correct class imbalance. Class imbalance must be addressed through data-level or algorithm-level strategies such as resampling, class weights, or appropriate evaluation design.

$$Precision = TP / (TP + FP)$$
$$Recall = TP / (TP + FN)$$
$$F1 = 2 \times (Precision \times Recall) / (Precision + Recall)$$

RESULTS AND DISCUSSION

Quantitative Synthesis of the Nine Studies

Tabel 3. Summary and Comparison of the Reviewed Studies on Deep Learning-Based IDS

Study	Architecture	Dataset	Preprocessing / Classification	Accuracy	Precision	Recall	F1
Sari et al. (2024)	Decision Tree, Random Forest, SVM	Network traffic	Supervised learning; comparative classifier evaluation	>95%	NR	NR	NR
Yu et al. (2024)	CNN/LSTM-oriented DL	Benchmark network intrusion data	Deep-learning NIDS	NR	NR	NR	NR
Odeh & Taleb (2024)	CNN, Autoencoder, LSTM	UNSW-NB15	Cleaning, normalization, feature selection; binary classification	99.89%	99.90%	99.88%	99.89%
Alharthi (2024)	CNN, LSTM, CNN-LSTM, ConvLSTM	KDD99, NSL-KDD, WSN-DS, CICIDS2017, Drone	Comparative DL evaluation; multi-dataset testing	99.99%*	99.99%*	99.99%*	99.99%*
Ataa et al. (2024)	CNN-LSTM, Transformer	InSDN	Cleaning, feature reduction, class merging	99.19%**	NR	NR	NR
Düzgün et al. (2024)	DL + transformer/NLP	UNSW-NB15, CIC-IDS2017, ISCX-IDS2012	Joint tabular and text/payload features	98.77%	85.94%	99.83%	92.37%
Kamal & Mashaly (2025)	Autoencoder-CNN, Transformer-DNN	CICIDS2017, NF-BoT-IoT-v2	ADASYN/SMOTE/ENN; binary and multi-class	99.96%***	99.96%***	99.96%***	99.96%***
Almuhanna & Dardouri (2025)	XGBoost, RF, CNN, LSTM, Autoencoder ensemble	CICIDS2017 + independent benchmark	Cleaning, feature engineering, SMOTE; 5-fold CV	≈100%	≈100%	≈100%	≈100%
Rotib et al. (2026)	RF, SVM, DBN, XGBoost, RNN-LSTM	CICIDS2017, NSL-KDD	KDD framework; preprocessing and feature engineering	98.10%	97.60%	98.20%	97.90%

** Highest reported ConvLSTM result in the cited study; **CNN-LSTM with six features; ***Transformer-DNN multi-class result on CICIDS2017. NR = not reported consistently enough in the accessible study text. Values are not pooled across datasets.*

The quantitative comparison changes the interpretation of the earlier manuscript. High performance is observed in several studies, but it is not uniform across all nine studies or all datasets. Therefore, the statement that hybrid models 'frequently boast accuracy above 95%' is replaced by the more defensible conclusion that several recent studies report accuracy above 95% under their respective experimental conditions, while other configurations and datasets produce lower values. The results of Ataa et al. (2024), Odeh and Taleb (2024), Alharthi (2024), Kamal and Mashaly (2025), and Almuhanna and Dardouri (2025) provide particularly strong evidence of high benchmark performance, but cross-study comparability remains constrained by dataset and protocol differences.

The table also shows why Accuracy alone is insufficient. Düzgün et al. (2024), for example, reported 98.77% Accuracy but a substantially lower Precision of 85.94% on UNSW-NB15, illustrating how a high overall accuracy can coexist with a less favorable false-alarm profile. Conversely, class-imbalance techniques such as SMOTE, ADASYN, ENN, and class weighting are preprocessing or learning strategies; F1-Score is an evaluation measure used to assess the resulting balance between Precision and Recall, not a remedy for imbalance itself.

Cross-study Patterns

1. RQ1: Architecture. The included studies show three recurring families: conventional deep classifiers (DNN/CNN), sequence-oriented models (LSTM/RNN), and hybrid/ensemble models. CNN is useful for local feature relationships, whereas LSTM/Transformer components are suited to sequential or contextual dependencies. Hybridization is therefore a recurring design response to heterogeneous network traffic.
2. RQ2: Preprocessing and imbalance. Cleaning, normalization, feature selection/reduction, and class balancing are common. Kamal and Mashaly (2025) explicitly combine ADASYN, SMOTE, ENN, and class-weight strategies, while Almuhanna and Dardouri (2025) use SMOTE after preprocessing. These studies reinforce the finding that preprocessing is part of the detection system, not a minor preliminary step.
3. RQ3: Performance. The evidence supports reporting Accuracy together with Precision, Recall, and F1-Score whenever possible. The revised table makes missing values visible rather than replacing them with inferred numbers. High results above 95% occur in multiple studies, but the evidence does not justify a universal superiority claim for hybrid models.
4. RQ4: Operational challenges. Across the literature, practical deployment is constrained by computational cost, dataset shift, class imbalance, latency, scalability, and interpretability. XAI-focused research further shows that high-performing IDS models can

P-ISSN: 2656-1743 |E-ISSN: 2656-1735
DOI: https://doi.org/10.34288/jri.v8i4.552
Accredited rank 4 (SINTA 4), excerpts from the decision of the DITJEN DIKTIRISTEK No. 230/E/KPT/2023

remain difficult for analysts to interpret (Mohale & Obagbuwa, 2025). Edge-oriented processing is particularly relevant to IoT and SDN because moving all detection to centralized infrastructure can increase latency.

5. RQ5: Synthesis. The recurring technical sequence across the nine studies is sufficiently stable to support a four-layer core pipeline: Data, Preprocessing, DL Model, and Evaluation. XAI and edge deployment are added as cross-cutting requirements because they address operational properties that cannot be assigned to only one layer.

Layer Conceptual Framework

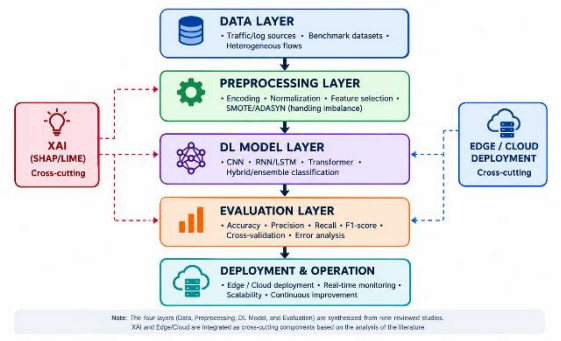

Figure 2. Conceptual framework derived from the recurring evidence across the nine included studies.

The four layers are not arbitrary. The Data Layer reflects the repeated use of benchmark or operational traffic sources. The Preprocessing Layer follows the repeated need for cleaning, normalization, feature reduction, and imbalance mitigation. The DL Model Layer represents the architecture choices documented across the studies. The Evaluation Layer reflects the repeated use of Accuracy, Precision, Recall, and F1-Score. XAI is positioned across the pipeline because explainability should accompany model outputs rather than be treated as a final-stage add-on. Edge/cloud deployment is also cross-cutting because latency and resource constraints influence data collection, model placement, and evaluation.

This framework extends the original manuscript by connecting model design to deployment requirements. In resource-constrained IoT or SDN environments, a lightweight model or edge execution may be preferable even when a larger centralized model has slightly higher benchmark accuracy. Similarly, XAI mechanisms such as SHAP or LIME can support analyst trust and incident investigation without changing the underlying classifier.

Limitations of the SLR

1. The original submission did not retain database export files or exact search-hit counts; consequently, the revised manuscript does not fabricate retrospective PRISMA counts.
2. The nine-study evidence set is small and heterogeneous. Several studies use different datasets, class definitions, train/test splits, and evaluation protocols, which limits direct numerical comparability.
3. Some included studies do not report all four requested metrics in a consistent form. These values are marked NR rather than estimated.
4. Most benchmark evaluations are laboratory-based; evidence for long-term deployment, concept drift, adversarial robustness, and production latency remains limited.
5. The conceptual framework is an evidence-derived synthesis and has not yet been experimentally validated as a deployed IDS.

CONCLUSIONS AND SUGGESTIONS

Conclusion

This revised SLR synthesizes nine recent peer-reviewed studies on DL-based network intrusion detection and strengthens the methodological transparency of the original manuscript. The evidence indicates that CNN, LSTM/RNN, Transformer, and hybrid/ensemble architectures are the dominant approaches, with hybrid designs frequently producing very high benchmark scores. Nevertheless, the review does not support a universal claim that hybrid models always exceed 95%; performance is conditional on dataset, preprocessing, class definition, and experimental protocol.

The synthesis yields a four-layer core framework Data, Preprocessing, DL Model, and Evaluation with XAI and edge/cloud deployment incorporated as cross-cutting requirements. This formulation directly links the reviewed evidence to practical concerns about class imbalance, model transparency, latency, scalability, and computational cost. The principal implication is that future IDS research should evaluate not only predictive accuracy but also generalization, minority-class detection, explainability, and deployment efficiency.

Suggestion

Future studies should validate the proposed framework using cross-dataset experiments, standardized train/test protocols, consistent reporting of Accuracy, Precision, Recall, and F1-Score, and explicit measurements of computational cost and latency. Lightweight DL and edge-based inference should be evaluated alongside XAI methods so that improvements in benchmark accuracy do not come at the expense of operational feasibility or analyst interpretability.

REFERENCES

Alharthi, R. (2024). Enhancing unmanned aerial vehicle and smart grid communication security using a ConvLSTM model for intrusion detection. Frontiers in Energy Research, 12, 1491332. https://doi.org/10.3389/fenrg.2024.1491332

Ali, A. H., Charfeddine, M., Ammar, B., Ben Hamed, B., Albalwy, F., Alqarafi, A., & Hussain, A. (2024). Unveiling machine learning strategies and considerations in intrusion detection systems: A comprehensive survey. Frontiers in Computer Science, 6, 1387354. https://doi.org/10.3389/fcomp.2024.1387354

Almuhanna, R., & Dardouri, S. (2025). A deep learning/machine learning approach for anomaly based network intrusion detection. Frontiers in Artificial Intelligence, 8, 1625891. https://doi.org/10.3389/frai.2025.1625891

Anis, F. M., Alabdullatif, M., Aljbli, S., & Hammoudeh, M. (2025). A survey on the applications of deep learning in network intrusion detection systems to enhance network security. IEEE Access, 13, 185357–185373. https://doi.org/10.1109/ACCESS.2025.3624952

Ataa, M. S., Sanad, E. E., & El-khoribi, R. A. (2024). Intrusion detection in software defined network using deep learning approaches. Scientific Reports, 14, 29159. https://doi.org/10.1038/s41598-024-79001-1

Chinnasamy, R., Subramanian, M., Easwaramoorthy, S. V., & Cho, J. (2025). Deep learning-driven methods for network-based intrusion detection systems: A systematic review. ICT Express, 11(1), 181–215. https://doi.org/10.1016/j.icte.2025.01.005

Düzgün, B., Çayır, A., Ünal, U., & Dağ, H. (2024). Network intrusion detection system by learning jointly from tabular and text-based features. Expert Systems, 41(4), e13518. https://doi.org/10.1111/exsy.13518

Kamal, H., & Mashaly, M. (2025). Enhanced hybrid deep learning models-based anomaly detection method for two-stage binary and multi-class classification of attacks in intrusion detection systems. Algorithms, 18(2), 69. https://doi.org/10.3390/a18020069

Mohale, V. Z., & Obagbuwa, I. C. (2025). A systematic review on the integration of explainable artificial intelligence in intrusion detection systems to enhancing transparency and interpretability in cybersecurity. Frontiers in Artificial Intelligence, 8, 1526221. https://doi.org/10.3389/frai.2025.1526221

Odeh, A., & Taleb, A. A. (2024). Robust network security: A deep learning approach to intrusion detection in IoT. Computers, Materials & Continua, 81(3), 4149–4169. https://doi.org/10.32604/cmc.2024.058052

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71. https://doi.org/10.1136/bmj.n71

Page, M. J., Moher, D., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). PRISMA 2020 explanation and elaboration: Updated guidance and exemplars for reporting systematic reviews. BMJ, 372, n160. https://doi.org/10.1136/bmj.n160

Rotib, A. A., Windasari, S., & Abdurohman, A. (2026). AI-powered intrusion detection system design for government data center infrastructure security. Jurnal Publikasi Ilmu Komputer dan Multimedia, 5(1), 309–319. https://doi.org/10.55606/jupikom.v5i1.6745

Sari, D. P., Halim, Z., Irlon, I., Waseso, B., & Saromah, S. (2024). Implementasi machine learning untuk deteksi intrusi pada jaringan komputer. Jurnal Minfo Polgan, 13(2), 1389–1394. https://doi.org/10.33395/jmp.v13i2.14074

Yu, J., Hu, J., & Zeng, Y. (2024). Deep learning based network intrusion detection. In W. Hong & G. Kanaparan (Eds.), Computer Science and Education (Communications in Computer and Information Science, Vol. 2023, pp. 125–136). Springer. https://doi.org/10.1007/978-981-97-0730-0_12

Wu, Y., Zou, B., Cao, Y., et al. (2024). Current status and challenges and future trends of deep learning-based intrusion detection models. Journal of Imaging, 10(10), 254. https://doi.org/10.3390/jimaging10100254

Zhang, Y., Muniyandi, R. C., & Qamar, F. (2025). A review of deep learning applications in intrusion detection systems: Overcoming challenges in spatiotemporal feature extraction and data imbalance. Applied Sciences, 15(3), 1552. https://doi.org/10.3390/app15031552

Yusuf, M. R., & Sumarlin, S. (2025). Penerapan deep learning untuk deteksi anomali dalam jaringan keamanan siber menggunakan recurrent neural networks (RNNs). Blend Sains Jurnal Teknik, 3(4), 460–470. https://doi.org/10.56211/blendsains.v3i4.800

Zeng, H., & Chen, H. (2024). Network intrusion detection based on LSTM. Frontiers in Science and Engineering, 4(9), 131–137. https://doi.org/10.54691/p4w71z56

Ruffo, V. G. da S., Lent, D. M. B., Komarchesqui, M., Schiavon, V. F., de Assis, M. V. O., Carvalho, L. F., & Proença Jr., M. L. (2024). Anomaly and intrusion detection using deep learning for software-defined networks: A survey. Expert Systems with Applications, 256, 124982. https://doi.org/10.1016/j.eswa.2024.124982