Contents lists available at www.journal.unipdu.ac.id
Register
Journal Page is available to www.journal.unipdu.ac.id/index.php/register

Research article

Machine and Deep Learning for Intrusion Detection: A PRISMA-Guided Systematic Review of Recent Advances

Hicham Zmaimita [a,*], *Abdellah Madani* [b], *Khalid Zine-Dine* [c]

[a,b] *Faculty of Sciences, Chouaib Doukkali University, B.P.299, Avenue Jabran Khalil, El Jadida, 24000, Morocco*
[c] *Faculty of Sciences , Mohammed V University, Avenue des Nations Unies, Agdal BP 8007.N.U, Rabat, 10000, Morocco*
email: [a,*] zmaimita.hicham@ucd.ac.ma, [b] madani.a@ucd.ac.ma, [c] khalid.zinedine@fsr.um5.ac.ma
* *Correspondence*

ARTICLE INFO

Article history:
Received May 12th, 2025
Revised June 14th, 2025
Accepted June 25th, 2025
Available online June 30th, 2025

Keywords:
Intrusion detection system
Machine learning
Deep learning
Network Security
Anomaly Detection

Please cite this article in IEEE style as:
H. Zmaimita, A. Madani, K. Zine-Dine, "Machine and Deep Learning for Intrusion Detection: A PRISMA-Guided Systematic Review of Recent Advances," *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 11, no. 1, pp. 66-74, 2025.

ABSTRACT

The massive increase in the number and complexity of cyberattacks has outgrown the capabilities of traditional Intrusion Detection Systems (IDS), driving a shift towards Machine Learning (ML) and Deep Learning (DL) solutions. This systematic literature review critically examines research published between 2020 and 2025 on ML and DL-based IDSs, focusing on model architectures, benchmark datasets, evaluation metrics, and key performance results. Adopting a rigorous methodology based on PRISMA 2020, 41 high-quality studies were selected and processed. The results reveal a clear preference for DL models, particularly Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), Bidirectional Long Short-Term Memory (BiLSTM) and hybrid ensembles, which achieve higher detection rates and greater robustness than traditional deep learning methods. However, persistent challenges such as data imbalance, high false positive rates, adversarial vulnerabilities, and real-time deployment constraints continue to prevent widespread adoption.

1. Introduction

The digital transformation of infrastructure and services has exponentially increased the volume and complexity of cyber threats targeting organizations and individuals. Intrusion Detection Systems (IDS) play an essential role in uncovering unauthorized access and malicious behavior within computer networks. Traditional IDS solutions, which are primarily based on predefined signatures or rule-based methods, struggle to detect unknown (zero-day) or obfuscated attacks and therefore have limited effectiveness in dynamic threat environments [1].

To overcome these limitations, security researchers have depended more on ML and DL techniques to enhance intrusion detection. ML algorithms, such as Support Vector Machines (SVM), Decision Trees and Random Forests, have shown excellent performance in detecting known attack signatures by learning from historical data **[2] [3]**. Meanwhile, DL models, such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Autoencoders have greater potential through automatic feature extraction from raw data and the ability to model complex temporal and spatial dependencies-[4] [5].

Considering the fast development and increasing number of contributions in this field, a systematic review is necessary to summarize recent advances, compare methods, and reveal research gaps. Previous surveys have either concentrated on certain particular techniques or lacked rigorous selection criteria, making it difficult to evaluate the current state of the art comprehensively [1] [5].

This paper provides a systematic overview of existing ML and DL-based intrusion detection and classification solutions, applying the PRISMA 2020 methodology and focusing on research published

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
11 (1) 2025 66-74

between 2020 and 2025. The objectives of this overview are to: (a) Provide background on intrusion detection systems; (b) Identify the most common ML and DL techniques used in IDS research; (c) Compare their performance with respect to evaluation metrics and datasets; (d) Highlight the current trends, challenges and potential future paths.

The rest of this document is organized as follows: Section 2 defines the role of Intrusion Detection Systems. Section 3 describes the systematic review process, including the search strategy and the inclusion and exclusion criteria. Section 4 presents the results of the selected studies and their analysis. Section 5 discusses the results, key challenges, and limitations of the research. Finally, Section 6 concludes the document by presenting future directions.

An IDS is a security mechanism that supervises network traffic, system activity, or both to detect suspicious behavior and potential attacks. When compromised activity is identified, the IDS sends alerts to system administrators and logs the events, providing them with the information needed to respond to the attack. In the era of global interconnection and rapid digital transformation, cyber threats have become increasingly sophisticated and frequent.

IDS are becoming increasingly important as traditional security measures are often unable to successfully detect or stop modern threats. There are two types of intrusion detection systems: host-based intrusion detection systems (HIDS), which operate at the individual system level, and network-based intrusion detection systems (NIDS), which monitor network traffic in real time. These systems rely on either known attack patterns or anomaly detection, which models normal behavior and reports any deviations. While signature-based methods are effective against known threats, they are ineffective against new or zero-day attacks. Anomaly-based systems, although more adaptive, often suffer from high false positive rates [6].

2. Materials and Methods

2.1. Methodology

This review was directed by the PRISMA2020 (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework, designed to ensure transparency, reproducibility and completeness in study selection and reporting [7].

2.2. Objective of the review

This review study aims to identify, analyze, and synthesize existing research on intrusion detection systems using ML/DL approaches. The objective is to provide a comprehensive understanding of current approaches, highlight their weaknesses, and suggest directions for future research.

2.3. Research Questions

The review is guided by the following research questions (RQs) enumerated in Table 1:

Table 1. Research questions

Questions	Motivation
RQ1: What are the most commonly used ML and DL techniques for intrusion detection and classification?	Identifying the most commonly used ML/DL techniques helps understand current trends, strengths and limitations in intrusion detection.
RQ2: What are benchmark datasets and evaluation metrics are employed to assess IDS performance?	Analyzing benchmark datasets and evaluation metrics ensures fair comparison, reproducibility and reliability of IDS research.
RQ3: What are the main challenges and future research directions in ML/DL-based IDS?	Investigating challenges and future directions in ML/DL-based IDS.

2.4. Search strategy

A comprehensive search was conducted across the following academic databases presented in Table 2.

Table 2. Compares the areas of expertise covered by a selection of databases.

Index	Database	URL
1	ScienceDirect	https://www.sciencedirect.com/
2	Google Scholar	https://scholar.google.com/
3	Web of science	https://clarivate.com
4	Scopus	https://www.scopus.com/
5	SpringerLink	https://link.springer.com/

The search included articles published in English between January 2020 and June 2025. The following Boolean query was used (with slight adjustments per database syntax): ("intrusion detection" OR "IDS" OR "cyberattack detection") AND ("machine learning" OR "deep learning").

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
11 (1) 2025 66-74

2.5. Inclusion and Exclusion Criteria

To ensure relevance and quality, articles were selected based on the following criteria:

Table 3. Inclusion and exclusion criteria

	Criteria description	Inclusion	Exclusion
IC1	Published between 2020 and 2025	X	
IC2	Published in English	X	
IC3	Peer-reviewed journal articles and conference proceedings	X	
IC4	Focus on ML or DL techniques for intrusion detection	X	
IC5	Include evaluation results on public or private datasets	X	
EC1	Non-English papers		X
EC2	Articles without experimental validation		X
EC3	General cybersecurity surveys without focus on ML/DL methods		X

2.6. Study Selection Process

2.6.1. First selection:

Duplicates were first removed, and the remaining records were screened by title and abstract to eliminate irrelevant entries, retaining only original research articles from peer-reviewed journals and conference proceedings.

2.6.2. Second selection:

To refine the selection, all chosen articles were subjected to a secondary review based on the eligibility criteria presented in Table 3, which were established in accordance with the research questions. These criteria ensured that the review focused exclusively on studies relevant to IDS implementation through ML and DL approaches.

The initial search yielded 200 articles. After removing duplicates, 149 records remained. Titles and abstracts were screened, maintaining 149 relevant articles. The application of a quality assessment (QA) further reduced this number to 87. A full-text review was then conducted, leading to a final selection of 41 studies that met all specified criteria.

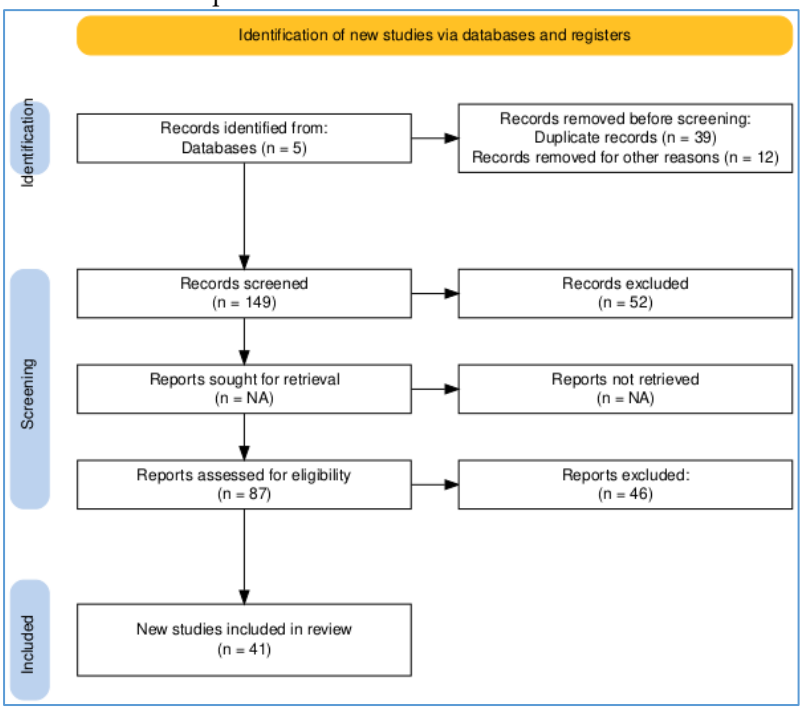

Fig. 1. PRISMA2020 flow diagram

2.7. Data extraction process

For each selected study, key information was extracted, including the year of publication, the type of ML or DL technique employed, the dataset used, the reported performance metrics (accuracy, F1-score, recall and precision), as well as the identified limitations and proposed directions for future work.

A structured data extraction table was developed and rigorously applied using Microsoft Excel to organize, manage, and extract relevant information from each eligible study.

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
11 (1) 2025 66-74

2.8. Quality Assessment (QA) checklist

High-quality systematic reviews require thorough literature searches and precision in reporting. A checklist was developed to assess the quality of each paper, with only those meeting the evaluation criteria included in the systematic review. A quality assessment of the selected papers was conducted following the application of the inclusion and exclusion criteria.

Table 4. PRISMA-based Quality Assessment Checklist

	Quality Assessment Criterion	Yes / No / Partial
Q1	Is does the study clearly focus on intrusion detection/classification using ML/DL?	
Q2	Is the research question or objective clearly stated?	
Q3	Is the dataset used for training/testing clearly identified and publicly available?	
Q4	Are the methods for training and evaluating the model clearly described?	
Q5	Is there a clear performance evaluation (accuracy, F1-score, etc.)?	
Q6	Does the study consider comparison with baseline or the latest advanced methods?	
Q7	Are were the limitations of the study discussed?	
Q8	Are the conclusions supported by the results?	

We evaluated the methodological quality of the included research papers applying a PRISMA-based Quality Assessment Checklist, as shown in Table 4. The checklist comprised eight criteria to assess clarity, reproducibility, dataset transparency, and robustness of performance evaluation. Each study received a score based on whether it fully met, partially met, or failed to meet each criterion.

3. Result and discussions

This section presents the principal outcomes of the selected studies, focusing on quantitative trends, model performance, datasets and techniques used. A total of 41 research papers were included in the final review following quality assessment and eligibility screening.

3.1. Distribution by Publication Year

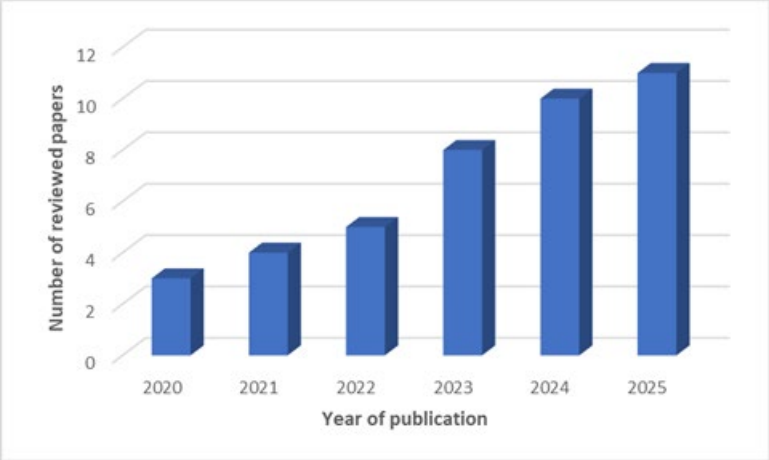

Fig. 2. Distribution of documents by year in this review

Fig. 2. illustrates the annual distribution of the analyzed papers. As shown, the number of publications addressing the reviewed topic has been steadily increasing, especially over the past six years (2020 and 2025). This trend highlights the rising interest in applying ML and DL approaches to intrusion detection, establishing it as an increasingly active area of research.

3.2. Distribution of papers by datasets

Based on our systematic review, the results, presented in Fig. 3, show an uneven distribution among the datasets used for intrusion detection. The majority of the datasets are represented only marginally, with just 2.08% for datasets like BIoT, CICDDoS2019, NF-ToN-IoT, NF-UQ-NIDS, SDN traffic, SIMARGL2021, UKM-IDS20, and UNR-IDD. In contrast, a few datasets dominate the distribution, particularly NSL-KDD (22.92%), CICIDS2017 (14.58%). It is evident that NSL-KDD, CICIDS2017, and UNSW-NB15 represent a significant portion of the data, with a combined total of 56.25% of the occurrences. This suggests that these datasets are widely adopted for IDS model studies and evaluations. As shown in Table 5, these datasets are popular due to their size, the diversity of attacks they cover, and their availability for research on intrusion detection.

 http://doi.org/10.26594/register.v11i1.5589

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
11 (1) 2025 66-74

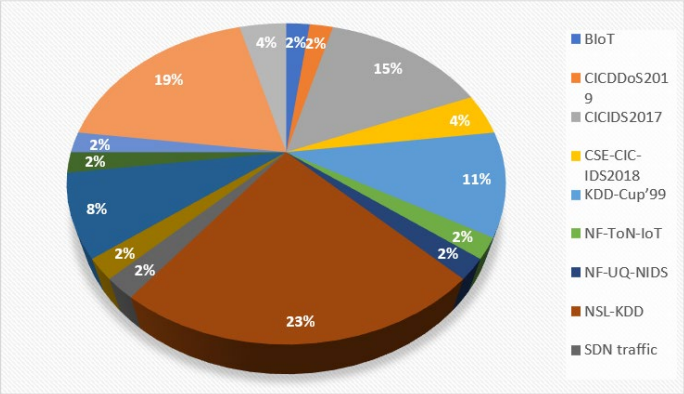

Fig. 3. Distribution of datasets analyzed in this review

Table 5. Comparison of datasets

Dataset	Number of Records	Type of Information	Year
KDD-Cup'99	5 million	Old network traffic	1999
NSL-KDD	125,000	Improved network traffic dataset	2009
CICIDS2017	3 million	Mixed network traffic	2017
CSE-CIC-IDS2018	4.7 million	Mixed network traffic	2018
CICDDoS2019	50 million	DDoS attack traffic	2019
NF-ToN-IoT	8 million	IoT logs (network, devices)	2020
NF-UQ-NIDS	2 million	Normalized network traffic	2020
SDN Traffic Datasets	500k–2M	SDN (Software Defined Network) traffic	2020
ToN-IoT	16 million	Multi-layered IoT logs (network, system, devices)	2020
UKM-IDS20	1–2 million	Modern IDS network traffic	2020
B-IoT	100,000	IoT network traffic	2021
SIMARGL2021	2–3 million	Mixed data: IoT, mobile, network	2021

3.3. Distribution of papers by methods:

In this subsection, we briefly review the selected papers, which are grouped according to the learning methods and categorized into two main groups: ML and DL. According to Fig. 4, DL methods are the most used by researches (64%), followed by ML (22%), a combination of ML and DL (7%), and Reinforcement Learning (RL) with 7%.

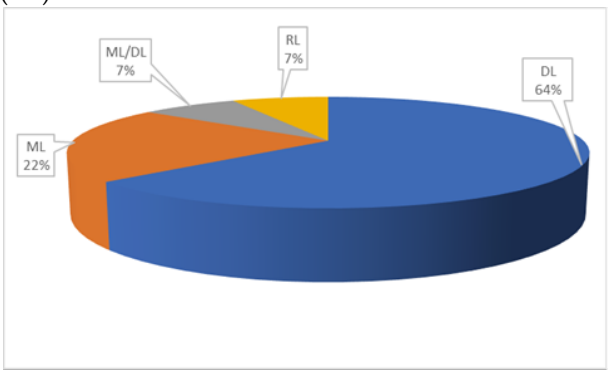

Fig. 4. Distribution document by methods

3.4. Overview of comparative results

A comparison of the reviewed studies highlights the significant progress made in intrusion detection using ML and DL techniques. Deep learning models, particularly CNNs, LSTMs, GRUs, BiLSTMs, and various hybrid architectures, have consistently demonstrated higher generalization capabilities and increased precision, with many achieving precision and recall scores exceeding 98%, and even reaching 100% in some specific cases [8], [9], [10], [11], [12], [13], [14], [15], [16].

Hybrid methods that integrate several models (DNN+GAN, Word2Vec+LSTM or ensemble techniques combining Random Forest, XGBoost, Adaboost, etc.) have shown remarkable effectiveness, demonstrating the strength of multi-model frameworks in handling complex intrusion scenarios [24], [30] and [25]. Recent work (2023-2025) using different datasets particularly CICIDS2017, UNSW-NB15, NSL-KDD, and ToN-IoT confirms this trend, often providing outstanding results in terms of accuracy, F1 score, precision, and recall [15], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30].

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
11 (1) 2025 66-74

3.5. Discussion

This review sets itself apart from previous studies in several key ways. First, it focuses exclusively on research published between 2020 and 2025, a period reflecting the most recent developments in intrusion detection, including the emergence of hybrid deep learning models, evolving benchmark datasets, and deployment-oriented concerns such as explainability and scalability. Second, the methodology follows the rigorous PRISMA 2020 framework, ensuring transparency, reproducibility, and a high standard of quality in study selection an approach not commonly adopted in earlier systematic reviews in this domain.

The frequent use of the NSL-KDD dataset, while somewhat dated, is justified by its structured design and widespread adoption, which enable consistent benchmarking across studies. Nonetheless, newer datasets such as CICIDS2017 and UNSW-NB15 are gaining traction due to their realistic traffic patterns and comprehensive attack coverage. Similarly, the predominance of models like LSTM, BiLSTM, and CNN in the literature can be explained to their architectural strengths: LSTM and BiLSTM excel at capturing sequential dependencies in time-series data, while CNNs are effective at extracting spatial features from traffic vectors. Their combination in hybrid architectures enables more robust and adaptive intrusion detection, accounting for their growing popularity in recent years.

The superior performance of specific models such as BiLSTM and hybrid deep learning ensembles can be attributed to their inherent architectural advantages in processing complex and high-dimensional intrusion data. Bidirectional Long Short-Term Memory (BiLSTM) networks, for instance, are particularly effective in modeling sequential dependencies by capturing both past and future context in network traffic. This bidirectionality enhances detection accuracy in scenarios where attack patterns unfold over multiple steps or sessions-a common characteristic in sophisticated, multi-stage intrusions.

Hybrid architectures that combine multiple models, such as CNN-LSTM, DNN-GRU, or ensemble frameworks integrating Random Forest and XGBoost, leverage complementary strengths. Convolutional layers (CNNs) efficiently extract local spatial features (e.g., packet structure, byte frequency), while recurrent layers (e.g., LSTM, GRU) capture temporal dynamics. This fusion allows hybrid models to generalize more effectively across different types of intrusions, especially those exhibiting both spatial and temporal anomalies.

From a theoretical perspective, these models can be analyzed through the lens of the bias–variance tradeoff. Deep neural networks with sufficient capacity (e.g., BiLSTM, CNNs) can significantly reduce bias by capturing complex intrusion patterns, but they also risk increased variance. Furthermore, understanding model behavior in IDS intersects with anomaly detection theory, particularly in relation to class imbalance and rare-event learning. Sequence-aware models like BiLSTM can adapt to temporal shifts and class transitions, making them more sensitive to anomalies that develop gradually or deviate from normal patterns over time.

Compared to the prior survey **[31]**, this review confirms the growing dominance of deep learning, particularly BiLSTM, CNN, and hybrid models, in intrusion detection, but differs in both scope and focus. While earlier reviews often emphasized architectural taxonomies or general trends, our analysis incorporates detailed performance metrics, dataset diversity, and deployment considerations. For instance, unlike broader surveys such as **[32]**, which review ML techniques across various cybersecurity domains, our work offers a focused and methodologically rigorous synthesis of ML/DL approaches applied specifically to intrusion detection systems.

Our study provides deeper operational insights that complement and extend the existing literature. Although many DL-based IDS models achieve high accuracy (>98%) under controlled conditions, real-time deployment remains constrained by computational overhead, inference latency, and limited adaptability in dynamic environments. These limitations highlight the importance of explainable AI, low-latency architectures and lightweight, robust models trained on realistic and diverse traffic data to bridge the gap between research and real-world application.

Beyond accuracy, several practical factors directly impact the deployment of ML/DL-based IDS. First, the computational complexity of deep models, especially BiLSTM and CNN-LSTM hybrids, poses challenges for real-time detection, particularly on edge or low-power devices. Second, the lack of explainability limits trust and adoption in critical infrastructures, where transparency is essential.

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
11 (1) 2025 66-74

SHAP, LIME or attention mechanisms should be further explored to address this gap. Third, supervised DL models often require large, well-labeled, and balanced datasets, which are difficult to obtain in real-world conditions marked by zero-day attacks and concept drift. Addressing these issues is essential for building next-generation IDS that are not only accurate but also trustworthy, efficient, and scalable.

4. Conclusion

The purpose of this systematic review is to analyze recent advances in IDS based on machine learning (ML) and deep learning (DL) techniques. A study of recent literature reveals a significant preference for deep learning architectures particularly CNN and LSTM, due to their enhanced capability to handle complex, high-dimensional, and unstructured data effectively.

The analysis shows that DL-based methods tend to achieve superior detection accuracy compared to classical ML techniques, especially for modern, large-scale datasets. However, these improvements usually come with a large computational load and depend on large-scale training data. Moreover, the lack of explainability and interpretability in many DL models remains a significant issue.

This paper makes several contributions by offering a qualified review of current methodologies, summarizing the state-of-the-art, and highlighting key research challenges such as inadequate evaluation of IDS models in real-time scenarios, the lack of standard performance metrics, and the low generalizability of models across a wide range of operational conditions.

This work contributes not only by synthesizing state-of-the-art techniques but also by identifying key research gaps related to operational feasibility, trust, and model robustness. Future research should focus on developing lightweight and interpretable models, enhancing real-time threat detection, improving dataset realism, and integrating explainable AI and adaptive learning mechanisms to better address evolving cybersecurity threats.

Author Contributions

H. Zmaimita: Conceptualization, data curation, formal analysis, investigation, methodology, project administration, resources, software, writing – original draft, and writing - review & editing. A. Madani: Conceptualization, project administration, resources, supervision, validation, visualization, writing – original draft, and writing – review & editing. K. Zine-Dine: Supervision, validation, visualization, and writing - review & editing.

Declaration of Competing Interest

We declare that we have no conflict of interest.

References

[1] H. Hindy *et al.*, 'A Taxonomy of Network Threats and the Effect of Current Datasets on Intrusion Detection Systems', *IEEE Access*, vol. 8, pp. 104650–104675, 2020, doi: 10.1109/ACCESS.2020.3000179.

[2] M. A. Ambusaidi, X. He, P. Nanda, and Z. Tan, 'Building an Intrusion Detection System Using a Filter-Based Feature Selection Algorithm', *IEEE Trans. Comput.*, vol. 65, no. 10, pp. 2986–2998, Oct. 2016, doi: 10.1109/TC.2016.2519914.

[3] T. Sowmya and E. A. Mary Anita, 'A comprehensive review of AI based intrusion detection system', *Measurement: Sensors*, vol. 28, p. 100827, Aug. 2023, doi: 10.1016/j.measen.2023.100827.

[4] Y. Ma, B. Niu, and Y. Qi, 'Survey of image classification algorithms based on deep learning', in *2nd International Conference on Computer Vision, Image, and Deep Learning*, F. Cen and B. H. Bin Ahmad, Eds., Liuzhou, China: SPIE, Oct. 2021, p. 9. doi: 10.1117/12.2604526.

[5] A. Kumar, A. Kumar, M. K. Singh, and P. Kumari, 'Cyber Attack Detection using Deep Learning', *Middle East Res J Engr Technol*, vol. 3, no. 04, pp. 44–50, Jul. 2023, doi: 10.36348/merjet.2023.v03i04.001.

[6] L. Diana, P. Dini, and D. Paolini, 'Overview on Intrusion Detection Systems for Computers Networking Security', *Computers*, vol. 14, no. 3, p. 87, Mar. 2025, doi: 10.3390/computers14030087.

[7] J. Burgert and G. C. Richards, 'Funding matters: time to update preferred reporting items for systematic reviews and meta-analyses?', *Journal of Clinical Epidemiology*, vol. 180, p. 111678, Apr. 2025, doi: 10.1016/j.jclinepi.2025.111678.

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
11 (1) 2025 66-74

[8] R. Dhahbi and F. Jemili, 'A Deep Learning Approach for Intrusion Detection', in *2021 IEEE 23rd Int Conf on High Performance Computing & Communications; 7th Int Conf on Data Science & Systems; 19th Int Conf on Smart City; 7th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys)*, Haikou, Hainan, China: IEEE, Dec. 2021, pp. 1211–1218. doi: 10.1109/HPCC-DSS-SmartCity-DependSys53884.2021.00186.

[9] N. Singh, S. Jaiswar, P. Jha, K. Virendra, V. Tiwari, and K. Saket, 'Adaptive Intrusion Detection Using Deep Reinforcement Learning: A Novel Approach', pp. 2455–6211, May 2024.

[10] J. Simon, N. Kapileswar, P. K. Polasi, and M. A. Elaveini, 'Hybrid intrusion detection system for wireless IoT networks using deep learning algorithm', *Computers and Electrical Engineering*, vol. 102, p. 108190, Sep. 2022, doi: 10.1016/j.compeleceng.2022.108190.

[11] V. Ravi, R. Chaganti, and M. Alazab, 'Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system', *Computers and Electrical Engineering*, vol. 102, p. 108156, Sep. 2022, doi: 10.1016/j.compeleceng.2022.108156.

[12] L. Zhang, K. Liu, X. Xie, W. Bai, B. Wu, and P. Dong, 'A data-driven network intrusion detection system using feature selection and deep learning', *Journal of Information Security and Applications*, vol. 78, p. 103606, Nov. 2023, doi: 10.1016/j.jisa.2023.103606.

[13] S. Hassen and A. Abdlrazaq, 'Contextual Deep Semantic Feature Driven Multi-Types Network Intrusion Detection System for IoT-Edge Networks', *ZJPAS*, vol. 36, no. 6, pp. 132–147, Dec. 2024, doi: 10.21271/ZJPAS.36.6.14.

[14] M. Abd Elaziz, M. A. A. Al-qaness, A. Dahou, R. A. Ibrahim, and A. A. A. El-Latif, 'Intrusion detection approach for cloud and IoT environments using deep learning and Capuchin Search Algorithm', *Advances in Engineering Software*, vol. 176, p. 103402, Feb. 2023, doi: 10.1016/j.advengsoft.2022.103402.

[15] Y. N. Kunang, S. Nurmaini, D. Stiawan, and B. Y. Suprapto, 'Attack classification of an intrusion detection system using deep learning and hyperparameter optimization', *Journal of Information Security and Applications*, vol. 58, p. 102804, May 2021, doi: 10.1016/j.jisa.2021.102804.

[16] M. Vishwakarma and N. Kesswani, 'DIDS: A Deep Neural Network based real-time Intrusion detection system for IoT', *Decision Analytics Journal*, vol. 5, p. 100142, Dec. 2022, doi: 10.1016/j.dajour.2022.100142.

[17] R. Devendiran and A. V. Turukmane, 'Dugat-LSTM: Deep learning based network intrusion detection system using chaotic optimization strategy', *Expert Systems with Applications*, vol. 245, p. 123027, Jul. 2024, doi: 10.1016/j.eswa.2023.123027.

[18] Y. Imrana, Y. Xiang, L. Ali, and Z. Abdul-Rauf, 'A bidirectional LSTM deep learning approach for intrusion detection', *Expert Systems with Applications*, vol. 185, p. 115524, Dec. 2021, doi: 10.1016/j.eswa.2021.115524.

[19] Y. Xue, C. Kang, and H. Yu, 'HAE-HRL: A network intrusion detection system utilizing a novel autoencoder and a hybrid enhanced LSTM-CNN-based residual network', *Computers & Security*, vol. 151, p. 104328, Apr. 2025, doi: 10.1016/j.cose.2025.104328.

[20] J. Fang and F. Leng, 'Network Security Intrusion Detection System Based on Deep Learning', *Procedia Computer Science*, vol. 261, pp. 1107–1113, Jan. 2025, doi: 10.1016/j.procs.2025.04.692.

[21] B. Xu, L. Sun, X. Mao, C. Liu, and Z. Ding, 'Strengthening Network Security: Deep Learning Models for Intrusion Detection with Optimized Feature Subset and Effective Imbalance Handling', *CMC*, vol. 78, no. 2, pp. 1995–2022, 2024, doi: 10.32604/cmc.2023.046478.

[22] M. Catillo, A. Del Vecchio, A. Pecchia, and U. Villano, 'A Case Study with CICIDS2017 on the Robustness of Machine Learning against Adversarial Attacks in Intrusion Detection', in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, Benevento Italy: ACM, Aug. 2023, pp. 1–8. doi: 10.1145/3600160.3605031.

[23] S. Asif, 'OSEN-IoT: An optimized stack ensemble network with genetic algorithm for robust intrusion detection in heterogeneous IoT networks', *Expert Systems with Applications*, vol. 276, p. 127183, Jun. 2025, doi: 10.1016/j.eswa.2025.127183.

[24] F. Alrayes, M. Zakariah, S. Amin, Z. Khan, and J. Alqurni, 'Network Security Enhanced with Deep Neural Network-Based Intrusion Detection System', *CMC*, vol. 80, no. 1, pp. 1457–1490, 2024, doi: 10.32604/cmc.2024.051996.

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
11 (1) 2025 66-74

[25] R. A. Abed, E. K. Hamza, and A. J. Humaidi, 'A modified CNN-IDS model for enhancing the efficacy of intrusion detection system', *Measurement: Sensors*, vol. 35, p. 101299, Oct. 2024, doi: 10.1016/j.measen.2024.101299.

[26] D. Suja Mary, L. Jaya Singh Dhas, A. R. Deepa, M. A. Chaurasia, and C. Jaspin Jeba Sheela, 'Network intrusion detection: An optimized deep learning approach using big data analytics', *Expert Systems with Applications*, vol. 251, p. 123919, Oct. 2024, doi: 10.1016/j.eswa.2024.123919.

[27] S. Shen, C. Cai, Z. Li, Y. Shen, G. Wu, and S. Yu, 'Deep Q-network-based heuristic intrusion detection against edge-based SIoT zero-day attacks', *Applied Soft Computing*, vol. 150, p. 111080, Jan. 2024, doi: 10.1016/j.asoc.2023.111080.

[28] B. Sharma, L. Sharma, C. Lal, and S. Roy, 'Explainable artificial intelligence for intrusion detection in IoT networks: A deep learning based approach', *Expert Systems with Applications*, vol. 238, p. 121751, Mar. 2024, doi: 10.1016/j.eswa.2023.121751.

[29] N. O. Aljehane *et al.*, 'Golden jackal optimization algorithm with deep learning assisted intrusion detection system for network security', *Alexandria Engineering Journal*, vol. 86, pp. 415–424, Jan. 2024, doi: 10.1016/j.aej.2023.11.078.

[30] A. Ba and M. Adda, 'Intrusion Detection in IIoT Using Machine Learning', *Procedia Computer Science*, vol. 251, pp. 265–272, 2024, doi: 10.1016/j.procs.2024.11.109.

[31] R. Kimanzi, P. Kimanga, D. Cherori, and P. K. Gikunda, 'Deep Learning Algorithms Used in Intrusion Detection Systems -- A Review', Feb. 26, 2024, *arXiv*: arXiv:2402.17020. doi: 10.48550/arXiv.2402.17020.

[32] R. Chinnasamy, M. Subramanian, S. V. Easwaramoorthy, and J. Cho, 'Deep learning-driven methods for network-based intrusion detection systems: A systematic review', *ICT Express*, vol. 11, no. 1, pp. 181–215, Feb. 2025, doi: 10.1016/j.icte.2025.01.005.