Review

Not peer-reviewed version

A Systematic Literature Review on Machine Learning for Intrusion Detection Systems

Ali Ahmed *, Ramy Mostafa, Mahmoud H. Qutqut *, Noha Ragab

Posted Date: 19 May 2026

doi: 10.20944/preprints202605.1231.v1

Keywords: intrusion detection system (IDS); machine learning (ML); ML-based IDS; deep learning (DL); systematic literature review (SLR); PRISMA; anomaly detection; cybersecurity

 doi:10.20944/preprints202605.1231.v1

Review

A Systematic Literature Review on Machine Learning for Intrusion Detection Systems

Ali Ahmed [1,*], Ramy Mostafa [1], Mahmoud H. Qutqut [1,2,*] and Noha Ragab [3]

[1] Center for Applied Mathematics and Bioinformatics (CAMB), Computer Science Department, Gulf University for Science & Technology, West Mishref, Hawally, 7207 Kuwait
[2] Faculty of Information Technology, Applied Science Private University, Amman, 11931 Jordan
[3] Independent Researcher, West Mishref, Hawally, Kuwait
* Correspondence: ali.aa@gust.edu.kw (A.A.); qutqut.m@gust.edu.kw (M.H.Q.)

Abstract

The use of Artificial Intelligence (AI) and Machine Learning (ML) in cybersecurity, especially for creating Intrusion Detection Systems (IDS), has become increasingly important. These systems are essential for detecting malicious behaviour, identifying network issues, and stopping cyberattacks in real time. Although extensive research has been conducted on various ML and Deep Learning (DL) models for IDS, the current literature remains incomplete. It has many different datasets, methods, and evaluation standards. As cyber threats become more advanced, it is crucial to conduct a thorough analysis of ML techniques for intrusion detection. The goal of this Systematic Literature Review (SLR) is to give a full picture of the most recent academic articles on ML-based IDS. The study addresses important research questions about the most widely used algorithms, the types of attacks and network environments covered, the methodological problems that remain unsolved, and the new trends that should shape future research. Following the PRISMA framework, we conducted a systematic review of peer-reviewed articles published between January 2022 and May 2025. We searched IEEE Xplore, ACM Digital Library, and SpringerLink, yielding 22,558 initial records. After carefully applying strict inclusion criteria, 125 papers were selected for the final analysis. We created a standardised data extraction form (i.e., using MS Excel) to gather bibliographic details, research emphasis, methodological strategies, datasets, evaluation criteria, and recognised constraints. We employed thematic analysis to develop a clear taxonomy. We identified five main research themes in our analysis: (1) ensemble and hybrid learning pipelines focused on performance optimisation (30 papers), (2) context-specific IDS designs for Internet of Things (IoT), cloud, and Software-Defined Networking (SDN) environments (34 papers), (3) data-centric engineering that deals with class imbalance and feature selection (20 papers), (4) deep neural architectures for representation learning (31 papers), and (5) trustworthiness concerns like adversarial robustness, zero-day detection, and Explainable AI (XAI) (10 papers). Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM), and Random Forests are the most commonly used algorithms, often combined. Nonetheless, significant deficiencies remain: about 2% of papers incorporate XAI, only 4% focus on adversarial robustness, and none validate their models in real-world production settings. Denial of Service (DoS) and Distributed DoS (DDoS) are the most common types of attacks in the literature, while Web attacks, ransomware, and advanced persistent threats remain poorly studied. The number of publications grows at an average of 30.2% annually, but the field still relies on legacy benchmark datasets rather than operational validation.

Keywords: intrusion detection system (IDS); machine learning (ML); ML-based IDS; deep learning (DL); systematic literature review (SLR); PRISMA; anomaly detection; cybersecurity

1. Introduction

Intrusion Detection Systems (IDS) are essential for organisational security, given the proliferation of connected devices these days [1]. IDSs are the cornerstone of today's networks, providing the

 doi:10.20944/preprints202605.1231.v1

primary mechanism for detecting unauthorised access, malicious payloads, and network anomalies [2]. However, the major problem is that cyberattacks become increasingly sophisticated. Thus, IDSs that use a standard signature-based detection method, which matches incoming traffic against a database of known attack signatures, are rendered ineffective, especially against zero-day and polymorphic attacks [3]. To address both vulnerabilities, the literature has shifted toward anomaly-based IDs powered by Artificial Intelligence (AI). Models such as Machine Learning (ML) and Deep Learning (DL) can automatically extract temporal and spatial features from high-dimensional network traffic flows, enabling the detection of subtle anomalies that signature-based approaches bypass [4]. Such a shift advanced the literature from focusing on reactive rule matching to proactive behaviour-based profiling. This also enables IDS to identify unusual patterns of activity rather than already reported threats. In ML-based IDS, the system defines a baseline for acceptable network behaviour. When live network traffic deviates from this baseline, the system flags it as an anomaly. Theoretically, this enables the detection of zero-day attacks. How ML-based IDS defines such a baseline is through training by automatically extracts features from raw network traffic and then training on that data. DL, like Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, can learn these patterns directly and map raw traffic to attack classifications without human feature engineering.

This paper presents a comprehensive Systematic Literature Review (SLR) of ML-based IDS research from 2022 to 2025 to investigate the current state of the literature and identify prevailing research themes. The motivation for this new SLR stems from the fact that, despite the high volume of research on ML-based IDS, the field seems to converge on highly repetitive practices! One observation about those practices is that they are prioritising theoretical benchmark performance over operational relevance. The majority of the research studies in this paper report near-perfect accuracy. Investigating such papers reveals that they heavily depend on a handful pool of overused, often outdated datasets. Legacy datasets such as KDDCup99 and NSL-KDD, created over two decades ago, continue to be used in the majority of study papers. This defeats the purpose of using them, since they bear no resemblance to modern attacks (e.g., attacks in modern networks such as the Internet of Things (IoT)). More critically, the literature is almost exclusively dataset-based, with the proposed models trained, validated, and tested on static CSV files, with no real-world deployment, validation, or even cross-dataset validation.

What prior SLRs, such as [5–7], lack is recency. These SLRs have become outdated since the domain is rapidly changing. In addition, current SLRs either cover a narrow subdomain or span older periods. They exhibit critical limitations in scope, timeliness, and analytical depth, as shown in Table 1. Hence, a new comprehensive review is urgently required to evaluate the new proposals, accurately map the domain's true state, and guide research toward resolving the current challenges. In this work, we make three key contributions listed below:

- A novel five-theme taxonomy that includes ensemble pipelines, context-specific designs, data-centric engineering, deep neural architectures, and trustworthiness to organise the fragmented literature.
- A detailed quantitative analysis of publication trends, dataset usage, and algorithmic preponderance.
- A critical synthesis determining ongoing methodological gaps, including the absence of real-world validation, adversarial robustness testing, and Explainable AI (XAI). This analysis serves as a guide for future work that prioritises research toward operational relevance.

 doi:10.20944/preprints202605.1231.v1

Table 1. Summary of SLRs on ML-based IDSs.

Work	Year	No. of Papers	Time Period	Focus	Key Limitations	How Our Review Addresse
[5]	2024	393	2018-2023	General IDS trends	Outdated (misses 2024-2025 surge); superficial taxonomy; no critical synthesis	Covers 2022-2025; provides deep thematic analysis with 5 themes
[6]	2024	21	2020-2023	Host-based IDS	Excludes NIDS; Insufficient sample; misses DL trends	Includes both NIDS/HIDS; 125 papers; comprehensive DL analysis
[7]	2024	32	2019-2023	ML algorithms for IDS	Small sample; descriptive only; ignores dataset over-reliance	Critical methodological critique; dataset analysis
[8]	2025	32	2014-2024	Network behaviour analysis	Restrictive scope; mixes obsolete and modern methods; no thematic mapping	Coherent 5-theme taxonomy; focused on recent advances

To this end, this SLR systematically explores the fragmented ML-based IDS landscape and addresses inflated performance claims through four research questions designed to uncover underlying trends, contexts, and operational limitations:

- **RQ1:** What ML and DL algorithms are most commonly employed in IDS research, and how are they merged? This would reveal the domain's methodological preferences and emerging architectures.
- **RQ2:** What attack types and network environments are addressed by current research work, and where are the critical coverage gaps? This determines areas of overemphasis or underemphasis regarding real-world cybersecurity threats.
- **RQ3:** What methodological challenges (such as real-world validation, reproducibility, and robustness testing) remain unaddressed? This exposes limitations and weaknesses that undermine operational relevance.
- **RQ4:** What are the emerging trends that characterise current ML-based IDS research, and what critical gaps should guide future investigations? This provides a roadmap for impactful research.

With these research questions guiding our study, the following section details the systematic methodology used to identify, search for, and synthesise the relevant literature.

The remainder of this article is structured as follows. Section 2 describes our research methodology (including the PRISMA framework), search strategy, and screening process. Section 3 presents descriptive analysis of the surveyed papers. We provide thematic synthesis organised in five themes in Section 4. Section 5 discusses our key findings and research gaps. Section 6 answers our research questions, and Section 7 concludes with future research directions.

2. Research Methodology

2.1. Systematic Literature Reviews (SLRs): PRISMA

An SLR must not only synthesise themes but also characterise the corpus itself. This study uses the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 methodology [9]. Generally, PRISMA is a well-known SLR methodology that provides a structured framework for collecting, assessing, and integrating research studies to ensure comprehensiveness, objectivity, and generalisability. PRISMA describes explicit steps for identifying, selecting, and analysing research studies in a precise workflow. This structured process minimises bias and ensures that only high-quality, relevant studies are included in the analysis.

 doi:10.20944/preprints202605.1231.v1

2.2. Search Strategy

To ensure a comprehensive and representative review, we search three major reputable digital libraries: IEEE Xplore, ACM Digital Library, and SpringerLink. We selected these databases for their extensive coverage of the computer science, ML, and cybersecurity literature. We deliberately chose not to restrict our search to specific journals or conferences, as the domain of ML-based IDS is rapidly evolving and producing impactful research from diverse venues. The search was conducted in May 2025 and was limited to publications from January 2022 to May 2025. The search strategy combined keywords related to ML, DL, and IDSs, along with their associated challenges. The following search queries were used:

- **IEEE Xplore (search in All Metadata)**
  ("machine learning" OR "deep learning") AND ("intrusion detection system" OR "IDS" OR "network intrusion detection") AND ("challenges" OR "limitations" OR "imbalanced dataset" OR "adversarial attack")
  Results: 200 papers retrieved from 2,648 total matches.
- **ACM Digital Library (search in Abstract):**
  ("machine learning" OR "deep learning") AND ("intrusion detection system" OR IDS OR "network intrusion detection") AND (challenges OR limitations OR "imbalanced dataset" OR "adversarial attack")
  Results: 100 papers retrieved from 120 total matches.
- **SpringerLink (search in full text):**
  ("machine learning" OR "deep learning") AND ("intrusion detection system" OR IDS OR "network intrusion detection") AND (challenges OR limitations OR "imbalanced dataset" OR "adversarial attack")
  Results: 1,000 papers retrieved from 19,790 total matches.

After initial filtering and before cross-database deduplication verification, we had 1,299 papers as the total number of initial records after removing duplicates within each source.

2.3. Inclusion and Exclusion Criteria

We included the studies that met the following criteria:

- Focus: Primary research on ML/DL-based IDS
- Publication type: Peer-reviewed journal articles or full conference papers
- Language: English
- Time period: Published between January 2022 and May 2025
- Methodology: Included empirical evaluation with acceptable experimental detail

We excluded studies based on the following criteria:

- Papers focused on cryptography, IoT, blockchain, malware, or computer vision, without an IDS application.
- Conceptual papers, or review articles that have no original empirical evaluation.
- Non-English publications
- Studies published before 2022
- Papers lacking sufficient methodological or experimental detail (e.g., unspecified datasets, missing performance metrics)

Our screening results are as follows, where n is the number of papers to review at each stage:

- Initial collection from databases: 22,558 papers
- Records removed after initial keyword and time filter: 21,259 (n = 1,299 papers)
- Duplicates removed: 1,011. After duplication removal: (n = 288 papers)
- Excluded after title/abstract screening: 162 papers (n = 126 papers).
- Excluded after full-text paper assessment: 1 paper (n = 125 papers).
- Final included papers: n = 125 papers.

 doi:10.20944/preprints202605.1231.v1

2.4. Screening Process

Following the database searches, all retrieved papers were exported to Zotero [1] reference manager, where duplicate entries were identified and removed using Zotero's duplicate detection service, followed by manual verification. The screening process involved two stages:

1. **Stage 1:** Title and abstract screen: two reviewers (RM, AA) independently scanned abstracts and titles for all non-duplicate publications. Publications were then classified as "exclude," "include," or "undecided." Publications classified as "undecided" by either reviewer proceeded to full-text review. Disagreements were settled through discussion or consultation with a third reviewer (MQ). The inter-rater agreement was substantial (Cohen's $\varkappa = 0.82$).
2. **Stage 2:** The same two reviewers assessed the potentially relevant publications independently against the inclusion criteria. The reviewers documented the reasons for exclusion at this stage.

After finalizing the list of included studies, details were transferred to a structured MS Excel sheet for systematic data extraction. The themes of the review were initially proposed manually through iterative discussion among all authors based on emergent patterns, then refined through collaborative reviews. The actual process is discussed in Subsection 2.4. It is worth mentioning that we employed AI-assisted text analysis tools such as DeepSeek [2] to verify the consistency of the manually identified themes. However, all final thematic decisions were made manually by the authors. Throughout the screening process, research team meetings were conducted to refine the inclusion/exclusion criteria and resolve unclear cases. Figure 1 presents the PRISMA flowchart of the screening phase, starting from the initial list to the final included publications. This process yielded 125 papers for final review, with 1 paper redacted during theme refinement (this exclusion is reflected in Figure 1).

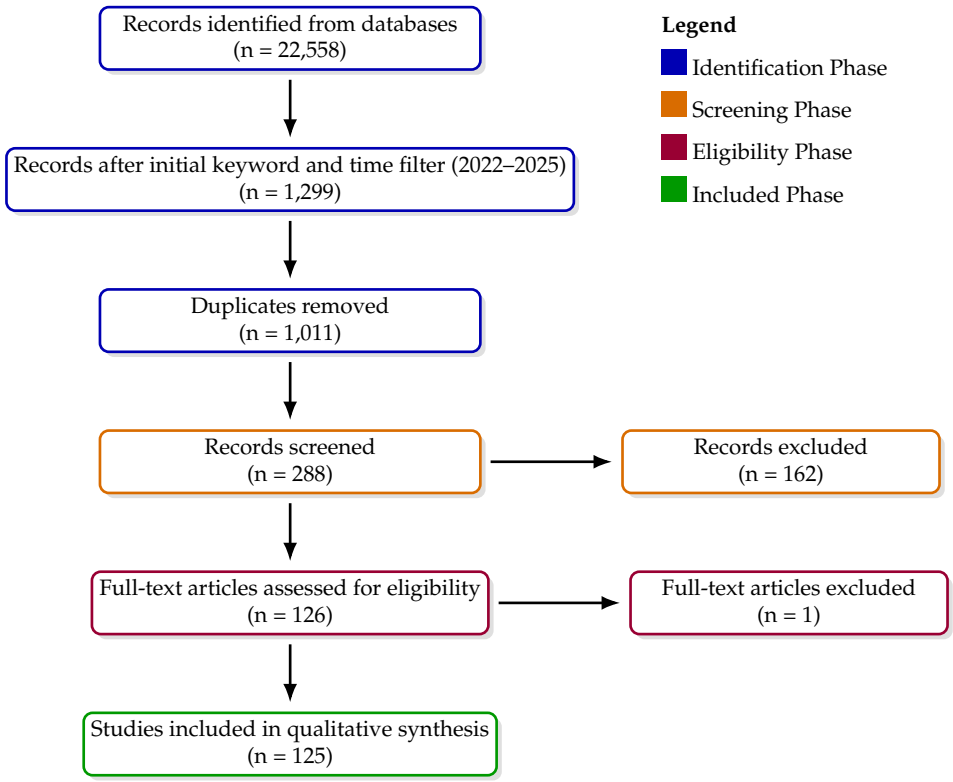

Figure 1. PRISMA flowchart of the SLR process.

2.5. Data Extraction

A standardised data extraction form was designed in Microsoft Excel and experimented on with five randomly selected papers to ensure consistency and completeness. After experimenting and

[1] https://www.zotero.org, last accessed 18 March 2026
[2] https://chat.deepseek.com, last accessed 18 March 2026

 doi:10.20944/preprints202605.1231.v1

minor refinements, one author (RM) extracted data from all 125 included papers, whereas a second reviewer (AA) independently verified a random sample of 25 papers (20% of the study papers) to ensure extraction accuracy. Any disagreements were resolved through discussion. The data extraction was done between December 2025 and February 2026, and extracted the following information:

1. **Bibliographic information:** Author names, year, publication venue, corresponding author country, and DOI.
2. **Research focus:** Primary goals, targeted attack types, and deployment environment (cloud, IoT, general networks, etc.).
3. **Methodological approach:** ML/DL algorithms used, feature selection strategies, handling of class imbalance, and use of XAI.
4. **Datasets and evaluation:** Dataset names and version, creation year, size, attack types covered, and listed performance metrics (accuracy, precision, recall, F1-score, and false-positive rate).
5. **Identified limitations:** Author's self-reported, including computational overhead, generalisation, and challenges with specific attack types.
6. **Reproducibility indications:** Whether code, datasets, or experimental details were made publicly available.

The extracted data were compiled into a master spreadsheet for use in the descriptive analysis and thematic synthesis.

2.6. Limitations of Methodology

While we conducted this review, there were several methodological limitations that should be considered when analysing its findings:

- **Publication bias:** This review, like all systematic reviews, is subject to publication bias; studies with statistically significant and positive results are more likely to be published than those with null findings or negative results.
- **Language bias:** Geographical biases due to the restriction to only English-language publications may exclude relevant research published in other languages, particularly from countries with strong cybersecurity research (e.g., China, Russia, and Japan).
- **Database coverage:** Even though we searched three main digital libraries (IEEE Xplore, ACM Digital Library, and SpringerLink), we did not include other databases. Some pertinent papers may have been skipped, particularly those published in venues not in these databases.
- **Timeframe constraint:** By limiting the review to 2022-2025, we include the most recent advances but exclude foundational papers that may still influence current research. Researchers should consult earlier reviews for historical context.
- **Primary study limitations:** The majority of the listed reviewed studies mainly rely on simulated datasets rather than real-world operational environments. This review synthesises findings from studies that may not reflect real-world IDS performance, which is a limitation we highlight as a major finding in our review.
- **Non-refereed literature exclusion:** We excluded non-refereed literature (technical reports, theses, and preprints) to maintain quality standards. However, this may miss novel approaches or negative results that appear first in these venues before formal publication.
- **Search term limitations:** Despite prudent search string design, some relevant papers may use alternative terms not captured by our keywords.

These limitations indicate that our findings may disproportionately reflect successful English-language research from indexed sources while inadequately representing poor outcomes, non-English studies, and innovative methodologies in the non-refereed literature. The actual condition of the field may be more varied and less consistently successful than depicted herein.

After establishing the systematic methodology, Section 3 provides a descriptive analysis of the reviewed papers, encompassing publication trends, geographic distribution, dataset usage patterns, and algorithmic prevalence.

 doi:10.20944/preprints202605.1231.v1

3. Descriptive Analysis

This section provides a descriptive analysis of publication trends, geographic distribution, dataset usage, and algorithmic frequency across the 125 reviewed studies. This establishes the quantitative foundation of the work, enabling readers to assess its currency and potential bias before diving into the thematic synthesis.

3.1. Publication Trends and Yearly Distribution

Analysing publication trends over time serves three critical purposes, namely, it validates the timeliness of this review, reveals the field's growth trajectory, and provides temporal context for interpreting the thematic patterns that follow. Figure 2 shows the distribution of the 125 included studies by year. The figure shows 19 papers were published in 2022, 28 in 2023, 36 in 2024, and 42 in 2025. This represents a compound annual growth rate (CAGR) and calculated by CAGR $= \left(\frac{\text{Ending Value}}{\text{Beginning Value}}\right)^{\frac{1}{n}} - 1 = \left(\frac{42}{19}\right)^{\frac{1}{3}} - 1 = 30.2\%$ over the four-year period, confirming sustained and increasing research interest in ML-based IDS. However, the year-over-year growth rates have steadily declined from 47.4% (2022-2023) to 28.6% (2023-2024) to 16.7% (2024-2025). This may indicate saturation with established methodologies and datasets, but we think the field is transitioning from rapid expansion (i.e., a new wave) to a more mature phase. The figure also indicates a linear trend fitted to the data ($R^2 = 0.99$) average annual increase of 7.7 papers. If we extrapolate, the result would be approximately 50 papers by 2026. However, this linear projection should be interpreted cautiously, as research activity rarely follows simple linear patterns indefinitely.

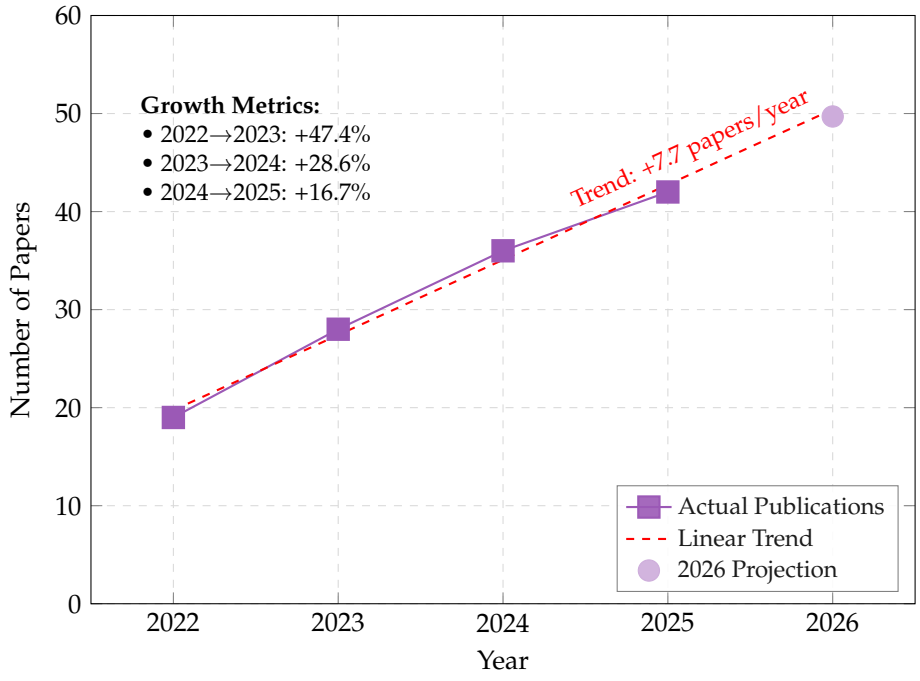

Figure 2. Number of ML-based IDS publications per year from 2022 to 2025.

3.2. Geographic Distribution of Research

The geographic distribution of research activity has implications for the diversity of perspectives. Figure 3 presents the geographic distribution of the 125 reviewed studies based on the first author's institutional affiliation. It is worth noting that this analysis is based on the first author's affiliation and does not capture international collaboration. Papers with first authors from one country may involve co-authors from multiple nations, potentially mitigating some concerns about geographic concentration.

India emerges as the dominant contributor with 52 papers (41.6% of the corpus), more than double the combined output of the next two countries. The United States follows with 19 papers (15.2%),

 doi:10.20944/preprints202605.1231.v1

and China with 16 papers (12.8%). Together, these three nations account for 87 papers (69.6%) of all reviewed studies, a substantial concentration of research activity. The remaining 30.4% of papers come from 18 other countries, demonstrating a global but highly uneven research landscape. India's substantial contribution likely reflects multiple factors: a large English-speaking research community, a significant government and industry investment in cybersecurity education and research [10], a growing IT sector with a strong security focus, and active publication in international venues. This concentration suggests that Indian researchers have become central to the field of ML-based IDS.

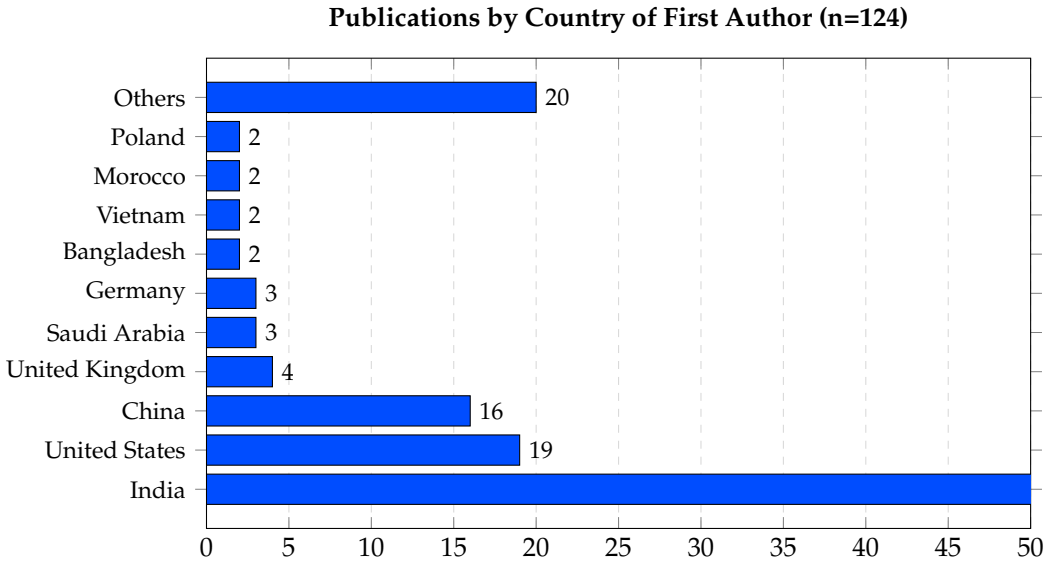

Figure 3. Geographic distribution of research by first author country.

3.3. Dataset Usage Analysis

Dataset selection fundamentally shapes the validity and generalisability of ML-based IDS research. We analyse dataset utilisation patterns across the 125 reviewed studies, focusing on popularity, temporal relevance, domain coverage, and implications for reproducibility. Figure 4(a) visualises these patterns, while Table 2 provides summary statistics. The three most frequently employed datasets are NSL-KDD (43 papers, 34.4% of all studies), CIC-IDS2017 (27 papers, 21.6%), and UNSW-NB15 (25 papers, 20.0%). Collectively, these three datasets appear in 95 papers (note that a single paper may use multiple datasets). This concentration raises concerns about database diversity. KDD Cup 99, despite being over two decades old, remains in use (14 papers, 11.2%).

The prominence of the NSL-KDD dataset, which represents network traffic and attack patterns from the late 1990s, is concerning. While NSL-KDD addressed some flaws in the original KDD Cup 99, it cannot represent modern network environments, traffic volumes, or attack methodologies. This constant use suggests the field may be optimised for historical benchmarks rather than modern threats. Another concern is that 17 papers (about 13.6%) either did not specify the dataset used or did not describe it. This hinders the reproducibility of the research findings.

Figure 4(b) shows the range of domains covered by the datasets used in the 125 reviewed studies. Most of the papers (85, 68%) use general network datasets like NSL-KDD, CIC-IDS2017, and UNSW-NB15. There are only 10 papers (8%) that examine IoT environments, 4 papers (3%) that examine industrial control systems, and 3 papers (2.4%) that examine Distributed Denial of Service (DDoS)-specific datasets. The other papers either leverage datasets from specialised fields, such as mobile networks or web traffic, or do not explicitly specify the application domain. This distribution emphasises the gap between real-world deployment environments and academic research. Unfortunately, this distribution reveals how dissimilar real-world settings are from those in academic studies.

 doi:10.20944/preprints202605.1231.v1

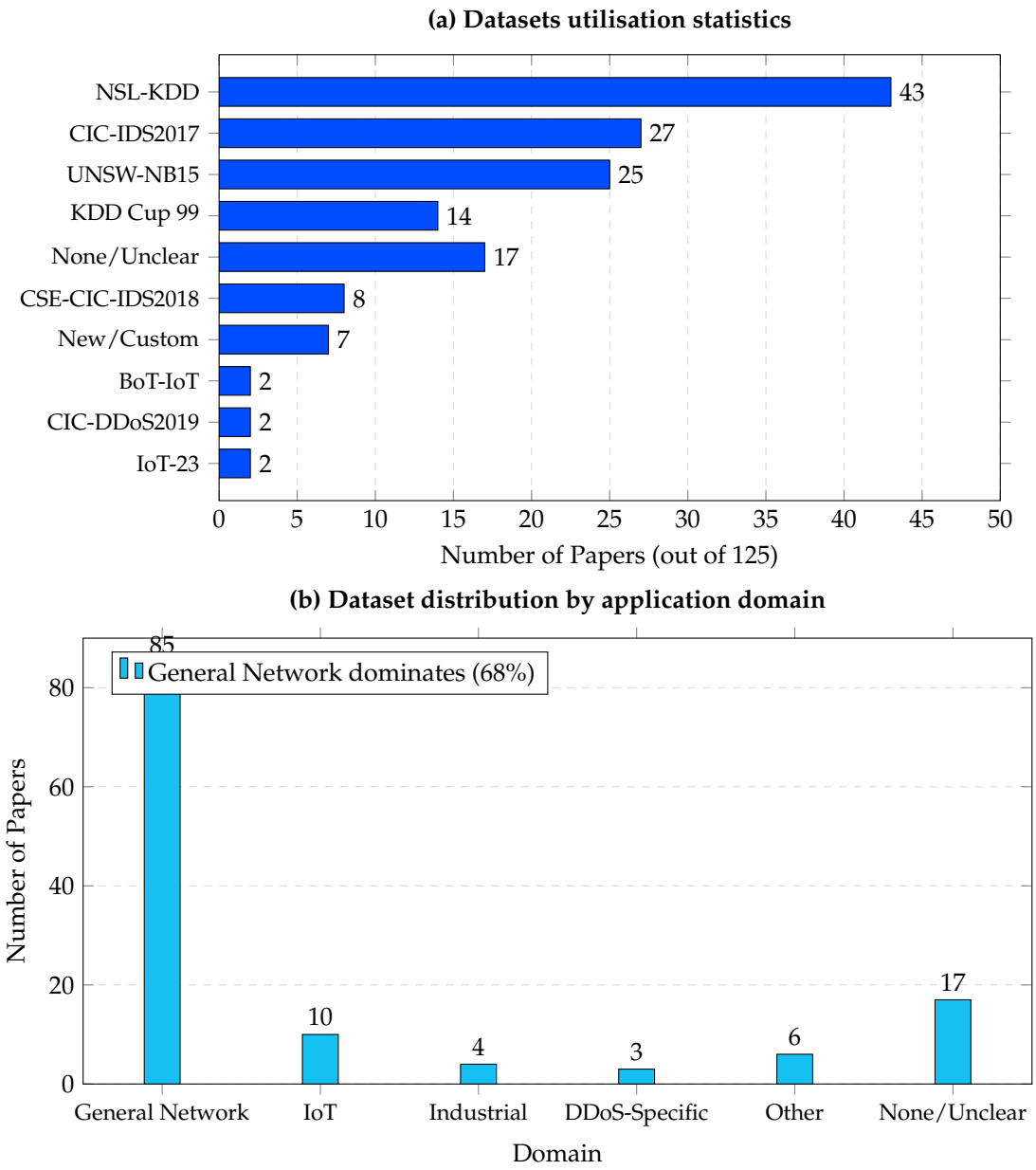

Figure 4. Dataset usage analysis distribution by domain in ML-based IDS research.

Table 2. Most Frequently Used Datasets

Metric	Count	Percentage
Papers using NSL-KDD	43	34.4%
Papers using UNSW-NB15	25	20%
Papers using CIC-IDS2017	27	21.6%
Papers using legacy datasets (KDD99/NSL-KDD)	57	45.6%
Papers using modern datasets (2015+)	73	58.4%
Papers with no/unclear dataset	17	13.6%
Total papers with specified datasets	**108**	**86.4%**

3.4. Algorithm Frequency Analysis

Understanding which algorithms dominate ML-based IDS research reveals the field's methodological preferences, evolving trends, and potential blind spots. Figure 5 presents the frequency of

 doi:10.20944/preprints202605.1231.v1

ML and DL algorithms across the 125 reviewed studies. Note that papers often employ multiple algorithms; each algorithm is counted independently whenever it appears in a study.

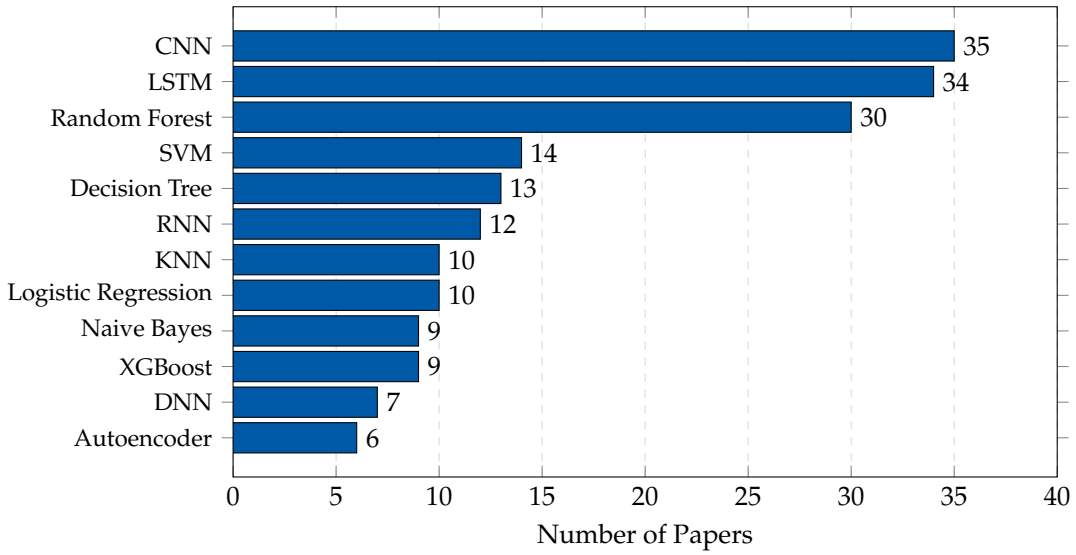

Figure 5. Algorithm Frequency Analysis.

The algorithmic landscape reveals that the DL architectures (i.e., CNN, LSTM, RNN, Autoencoders, DNN) collectively appear in 109 papers (87.2%) of all studies, while traditional ML methods (i.e., Random Forest, SVM, Decision Tree, KNN, Naive Bayes, and Logistic Regression) appear in 86 papers (68.8%). Note that these categories are not mutually exclusive, as many papers employ both DL and traditional ML techniques. The overlap indicates that the field has not fully shifted to DL but rather maintains a pluralistic approach.

The nearly equal number of papers on CNNs (35) and LSTMs (34) demonstrates the field's mature understanding that intrusion detection requires both spatial analysis (i.e., what is in each packet) and temporal analysis (i.e., how packets relate over time). This understanding has driven the popularity of hybrid CNN-LSTM architectures, as we will discuss later on. Also, the low number of transformer-related papers represents a significant research opportunity. Given their success in capturing long-range dependencies in sequences, transformers could potentially outperform LSTMs for intrusion detection, particularly for attacks that unfold over extended periods. The combination of transformers and explainability techniques (e.g., attention visualisation) could also address interpretability concerns.

4. Thematic Synthesis

This section is structured around a five-theme taxonomy that emerged inductively from iterative coding and clustering of study characteristics during thematic synthesis of the 125 papers. Theme 1 (Section 4.1) and Theme 4 (Section 4.4) are algorithm-centric, exploring the ensemble/hybrid learning pipelines and deep neural architectures, respectively. Theme 2 (Section 4.2) shifts the focus to the computational environment, examining how IDS designs are customised for IoT, cloud, and SDN environments. Theme 3 (Section 4.3) adopts a data-centric view by highlighting how data engineering, feature selection, and class imbalance drive performance. Finally, Theme 5 in Section 4.5 addresses the critical challenge of trustworthiness, covering adversarial robustness, zero-day detection, and XAI.

4.1. Theme 1: Ensemble and Hybrid Learning Pipelines Aimed at Performance Optimisation

This theme discusses a popular stream of research like ensemble methods and hybrid architectures. A hybrid architecture encompasses different learning paradigms to improve detection performance. The theme shows how the field moved from a single model to a more complex hybrid one.

 doi:10.20944/preprints202605.1231.v1

4.1.1. Tree-Based Ensembles and Boosting Methods

Tree-based ensemble methods such as Random Forest, XGBoost, and LightGBM provide strong baselines and consistently up-to-date performance. These methods remain highly competitive in terms of interpretability and efficiency. Gradient boosting methods have been improved to address problems such as class imbalance, insufficient data, and the presence of extra features. Under this theme, there are quite a few proposals. For example, tree-only methods like [11] propose classifiers with a small number of important features and evaluate them on the CSE-CIC-IDS2018 dataset using Random Forest and Decision Tree algorithms. For most studied attacks, tree methods are superior. It is noted that infiltration attacks are difficult to detect because there are few samples of them.

Building on the theme of generative and DL models, [12]'s GMM-WGAN-IDS system combines an autoencoder, Wasserstein GAN with Gaussian mixture modelling, and CNN-LSTM for classification. The model outperforms state-of-the-art methods on NSL-KDD and UNSW-NB15. The authors note a key limitation is that the model suffers to generalise to new environments, which aligns with concerns about real-world deployment raised earlier. Another work that falls under the same umbrella is [13], which combines SVM and Random Forest. The proposed SVM-RF hybrid model outperforms individual models, achieving 99.1% accuracy on a custom dataset with more than 1.7 million entries. Although it has been retracted, the work in [14] combines fuzzy logic with ML. However, the authors acknowledge generalisation concerns, questioning performance in different network environments.

The work by [15] evaluates classic ML (RF, SVM, etc.) on the KDD Cup 1999 Dataset. DoS detection ranges from 98.79% to 99.81%, Probe from 96.34% to 99.64%, R2L between 96.15% and 98.66%, and U2R from 79.98% to 99.73%. The study concludes that rare attacks remain challenging despite effective feature selection. Shifting focus to a comparative analysis, [16] evaluates Gradient Boosting and Random Forest on the NSL-KDD dataset, achieving 100% accuracy. To validate these findings, the authors recommend extending the work to include additional datasets and real-world testing environments.

A recent work by [17] built a hybrid CNN-RNN architecture that combines a CNN for spatial features and an RNN for temporal patterns. On the NSL-KDD dataset, it achieves 98.5% accuracy and 97.8% precision against multiple attacks. Performance varies with datasets, and real-time use remains untested. Moving from single ensembles to heterogeneous combinations, the authors of [18] build a diverse ensemble combining 1D CNN, FT-Transformer, and XGBoost. The approach leverages the strength of different models to detect varied patterns for better coverage. Across four datasets, it performs well on all metrics, though scalability remains a concern for larger deployments.

In summary, tree-based ensembles remain widely used today and promise to perform well [19]. Boosting methods, on the other hand, are more accurate and can be used in a variety of situations, such as protecting vehicles and networks from intruders. Tree-based ensembles usually consume less time to train and are easier to understand than DL models.

4.1.2. Hybrid Deep–Classical Pipelines

The shift to hybrid models is one of the most intriguing developments in recent IDS research. Researchers use both DL for representation learning and classical ML for classification, rather than choosing only one. When used together, they often work better than when used alone. For instance, taking a different optimisation approach, the work in [20] combines Butterfly optimisation with deep metric learning to separate normal and abnormal behaviours. Tested on UNSW-NB15 and NSL-KDD, it achieves 99% accuracy across various attack types but, like many other models, struggles with novel threats that fall outside its training distribution.

[21] builds a multi-agent system that learns as traffic changes, using continual deep anomaly detectors with federated learning. It scores flows with attack probability. Tested on CIC-IDS2017 and CSE-CIC-IDS2018, CNN models achieve 95% detection with 128 flows per update. LSTM models detect intrusions within 15 packets, though complex attacks remain challenging. A recent work by [22] examined a hybrid framework that used the CICIDS2018 dataset to analyse DoS, U2R, R2L, and

 doi:10.20944/preprints202605.1231.v1

probing attacks. The results are promising with 99.98% accuracy, 97.5% precision, and 96.8% recall. This outperforms traditional models. The main concern is that the model needs to be tested on a modern dataset to validate it.

Hybrid models consistently outperform single-model approaches. However, the increased complexity associated with hybrid models is a significant consideration. Enhanced accuracy often results in slower and more resource-intensive systems.

4.2. Theme 2: Context-Specific IDS Design (IoT, Cloud, SDN Environments, etc.)

The second major theme captures the growing recognition that intrusion detection solutions must be tailored to specific deployment contexts. Rather than proposing one-size-fits-all models, researchers increasingly design context-aware systems that account for the unique constraints and requirements of different environments. For instance, to extend the current approaches to critical infrastructure, the authors of [23] develop IGWO-GRU for industrial control systems by combining an improved grey wolf optimiser with GRU. They test on the pipeline and SWaT datasets; it improves accuracy but requires testing across a more diverse set of systems to validate its broader applicability.

4.2.1. IoT Intrusion Detection Under Constraints

The IoT and Industrial IoT environments present distinct challenges compared to traditional networks [24]. Devices in these environments often have limited power, memory, and processing capabilities. They employ a variety of protocols. In industrial contexts, security breaches can result in tangible physical consequences. Research within this sub-theme focuses on designing IDS models that balance detection accuracy with computational efficiency. For example, [25] studies wireless sensor networks, which form the sensing and data acquisition layer of the IoT ecosystem. The work uses Recursive Feature Elimination (RFE) with resampling and is evaluated on the NSL-KDD dataset against DoS, Probe, U2R, and R2L attacks. Their proposed model achieves 99.78% accuracy for DoS using Random Forest with fewer features. The authors note that more testing is needed on other datasets.

[26] introduces a Deep Convolutional Neural Network (DCNN) for intelligent network systems. The model achieves 99.5% accuracy on CICIoT2023 for binary classification, with higher results using other datasets, including CICIDS-2017 and CICIoMT2024. The authors test DDoS, DoS, Mirai, and web-based threats, noting that some minor attack classes are harder to detect. [27] evaluates a hybrid CNN-BLSTM model called BLoCNet on CIC-IDS2017, IoT-23, Bot-IoT, and UNSW-NB15. The results show 98% accuracy using CIC-IDS2017, 99% using IoT-23, but 76.34% using UNSW-NB15. Yet, the authors acknowledge that underrepresented attacks remain problematic and suggest a focus on improving the detection of minority classes. Along the same research line,

[28] presents AIDINN-CSD, a framework combining preprocessing and optimisation to detect anomalies in IoT networks. Tested on the CIC IoT 2022 dataset, it achieves 99.23% accuracy and 98.97% precision, surpassing existing methods. However, the authors note its complexity and seek future improvements in efficiency. [29] explores running an IDS on ESPaper 32, a microcontroller with 8 KB SRAM. Testing SNN, RNN, and DRNN models on the NSL-KDD dataset, the SNN performs best, achieving 94.04% precision and 0.226 ms inference time, fitting in 8 KB. Nonetheless, the authors propose reinforcement learning improvements and real-world IoT environment testing.

[30] targets sinkhole attacks in IoT networks. Their edge-assisted system (EaHIDS) uses a hidden Markov model to identify malicious nodes. Tested on simulators and testbeds, accuracy ranges from 94.12% to 98.49%. Despite this, the authors note scalability concerns and identify future work on mixed attack detection. To address the need for efficient deployment, [31] develops compact autoencoders specifically designed for edge devices and compares Vanilla, Deep, and Convolutional variants. The Convolutional Autoencoder (CAE) achieves 96% accuracy on university network data and 99.94% on CSIC 2010, while using significantly fewer parameters. However, the authors caution that performance depends critically on optimising the parameter α.

 doi:10.20944/preprints202605.1231.v1

Several key observations emerge from the analysis of this sub-theme. Firstly, several studies demonstrate that high detection accuracy is achievable in IoT environments. However, it often entails trade-offs such as increased complexity, higher memory consumption, or diminished performance in detecting rare attacks. Secondly, the deployment of these solutions in real-world scenarios remains an exception rather than the norm. A significant number of studies rely on standard datasets for testing, rather than actual IoT hardware. Thirdly, the field is a trajectory towards developing lightweight models capable of operating on resource-constrained devices, as exemplified by studies such as [29].

4.2.2. SDN/Cloud-Conditioned IDS

SDN and cloud environments are a double-edged sword for intrusion detection [32]. On the one hand, they offer centralised control and better visibility into network traffic. On the other hand, they introduce new attack surfaces and scalability headaches. Research in this section tries to balance these trade-offs. Generally, ML-based IDS enhances detection of network attacks in SDN environments, achieving high accuracy with faster threat response [33]. Selecting appropriate models, feature selection, and scalable architectures are crucial for balancing detection performance with computational efficiency in deployments.

For example, [34] targets Slow-Read DDoS and DNS tunnelling attacks. Their multi-layer stacking ensemble achieves a 0.99% F1 score and a 0.001% false-positive rate on corporate networks, outperforming deep neural networks, though it requires more resources. [35] presents an adaptive ensemble framework using PSO that outperforms older approaches on the NSL-KDD and CICIDS datasets, achieving higher accuracy. To protect against DDoS attacks in SDN, [13] combines SVM and Random Forest. Their SVM-RF hybrid model outperforms individual models, achieving 99.1% accuracy on a custom dataset with more than 1.7 million entries. The main issue with this work is the limited threat models. [36] takes boosting in a new direction by using XGBoost to protect connected vehicles. Their IDS for Vehicular Ad Hoc Networks (VANETs) is based on Software-Defined Networking (SDN) and tests for three types of threats: DoS, fuzzy attacks, and RPM spoofing. The results are amazing: 99.89% accuracy for DoS attacks and 99.93% accuracy for both fuzzy and spoofing attacks. Compared to current systems using KNN or LSTM-AE, that is a clear win. However, the authors did not exaggerate their assertions, as their dataset is limited to car-hacking scenarios. They say that using it in the real world would mean dealing with many more threats, such as insider attacks and zero-day exploits. They say that the next big step is to test outside of the lab.

[37] proposes a hybrid framework for SDN environments. On the InSDN dataset, it achieves 95% accuracy across DoS, U2R, R2L, and probing attacks. The model achieves a precision of 97.5% and a recall of 98.2%. But the authors are careful not to overpromise. They note that performance may vary across datasets, and they want future work to address real-time processing and transfer learning. The goal is to build models that adapt, not just perform well on one benchmark.

A range of recent studies has proposed innovative ML solutions for intrusion detection in cloud and network environments, each with distinct strengths and areas for future work. For instance, [38] employs a multi-stage architecture using MASNet for feature extraction, a Binary Artificial Rabbit Optimiser for selection, and IGhostTaV2Net for classification, achieving an impressive 99.82% accuracy against DDoS attacks. However, the paper's reliance on an unnamed dataset makes direct comparison difficult, a limitation the authors acknowledge by suggesting broader testing. Similarly, addressing detection efficacy, [39] focuses on building an efficient cloud IDS through ML and dimensionality reduction. Tested on the widely-used CSE-CIC-IDS2018 dataset, this model effectively detects a range of threats, including hypervisor attacks, U2R, and DoS, with a high detection efficiency of 99.31% and an accuracy of 92.03%. Despite these strengths, a precision of 78.25% indicates that false positives remain a concern, prompting future work to expand attack coverage and refine performance.

Other researchers have explored ensemble methods to bolster detection rates. The EICDL ensemble model from [40] was tested on legacy datasets such as KDDCup 1999, UNSW-NB15, and NSL-KDD, achieving a recall of 92.14%. The authors acknowledge the inherent challenges in protecting cloud VMs and recommend combining different learning and classification models as a promising path forward.

 doi:10.20944/preprints202605.1231.v1

Finally, shifting focus to a comparative analysis, [16] evaluates Gradient Boosting and Random Forest on the NSL-KDD dataset, achieving 100% accuracy. To validate these findings, the authors recommend extending the work to include additional datasets and real-world testing environments.

Several patterns appear from the analysis of this sub-theme. Firstly, accuracy demonstrates significant variability, ranging from 62% to 99.8%, indicating the critical importance of dataset selection and model choice. Secondly, numerous studies continue to utilise older datasets, such as NSL-KDD, despite the availability of more recent alternatives. Thirdly, a common conclusion across nearly all studies is the recommendation to test on a broader range of data, encompassing a wider array of attacks, and advance towards real-world implementation.

4.3. Theme 3: Data-Centric Engineering as a Primary Driver of IDS Performance

This theme reflects a paradigm shift in the literature. Increasingly, researchers recognise that data quality, representation, and engineering are as important as algorithmic sophistication. The theme encompasses papers that focus on how data is collected, processed, augmented, and represented.

4.3.1. Imbalance-Aware Intrusion Detection

Class imbalance is one of the oldest and most persistent problems in intrusion detection. Normal traffic always dwarfs attack traffic, sometimes by huge margins. Models trained on such data tend to get good at spotting normal behaviour but miss the designated attacks they are supposed to catch. The papers introduced in this section tackle this problem head-on, using a mix of sampling techniques, generative models, and smart preprocessing. Moving beyond traditional ML, [41] combines improved spotted hyena optimisation (ISHO) and honey badger algorithm (HBA) with the SE-ResNet152 deep learning architecture. Tested on UNSW-NB15, CSE-CIC-IDS2018, and CICIDS2019, it achieves over 99% across key metrics, though the authors acknowledge that runtime remains a concern for practical deployment.

[42] compares the speed and accuracy of Random Forest and Boosting. On the NSL-KDD dataset, their Boosting framework detects DoS, Probe, U2R, and R2L attacks with 99.03% accuracy. Its longer training period limits its real-time application, even though it is more effective than other approaches at handling minority classes. Hence, the authors suggest exploring hybrid approaches to overcome this limitation.

Moving from detection to handling class imbalance, [43] specifically addresses rare attacks using weighted SMOTE balancing and Particle Swarm Optimisation. Tested on UNSW-NB15, detection rates for rare attacks improve from 22.61% to 39.68%, though the authors caution that SMOTE can introduce noise into the training data. [44] combines SVMSMOTE oversampling with CNN and uses Random Forest for feature selection. Tested on CIC-IDS2017, the model achieves 97.91% accuracy and 97.88% true positive rate, with just 1.58% false positives. It performs well across DoS variants, web attacks, infiltration, and Heartbleed, though it struggles with new attacks. The authors suggest transfer learning for novel threats.

To address classification challenges, the DSSTE framework in [45] introduces a novel approach that separates hard-to-classify samples from easy ones. Tested extensively on CSE-CIC-IDS2018 and NSL-KDD against 24 techniques, it achieves 81.6% accuracy on NSL-KDD and a much stronger 96.8% on CSE-CIC-IDS2018. However, the authors acknowledge that multiclass classification remains challenging, highlighting the need for future work on feature extraction to address this gap. To address both class imbalance and multiclass performance, [46]'s AGM framework combines ADASYN sampling with GMM for data balancing and uses C3BANet for classification. On UNSW-NB15, detection rates reach an exceptional 99.99% for binary tasks and 96.82% for multiclass, with similarly impressive results on CICIDS2017 (99.78% and 99.57%). Despite these strong metrics, the model's complexity raises concerns about overfitting for real-time deployment, a cautionary note that echoes the generalisability issues observed in other sophisticated IDS approaches.

The unifying theme of these papers is threefold. Firstly, the issue of imbalance is not merely peripheral; it is fundamental to IDS research, and these studies demonstrate significant advancements

 doi:10.20944/preprints202605.1231.v1

in this area. Secondly, handling imbalances is increasingly integrated into deep learning architectures, incorporating techniques such as Generative Adversarial Networks (GANs), autoencoders, and attention mechanisms. Thirdly, while achieving high scores on benchmarks, the true test lies in real-world applicability. Almost every paper concludes with a recommendation for further empirical validation beyond laboratory settings.

4.3.2. Data Engineering and Representation Enhancement

In some cases, difficulty lies in the data provided rather than the model used. When attack samples are scarce or datasets are small, even the best algorithms struggle. That is where data augmentation comes in. By creating synthetic training data, researchers can give their models more data to learn from. The papers in this section explore different ways to do this.

Addressing the need for more adaptable systems, [47] develops DLC-IDS, a hybrid framework blending signature-based and anomaly-based detection. The system uses a central multi-class classifier supported by subordinate classifiers, implementing CTGANs for synthetic samples and LSTM with self-attention for novel attacks. Tested on NSL-KDD and gas pipeline datasets, DLC-IDS shows high accuracy and low false negatives; still, the authors note that scalability remains a concern for larger, more diverse deployments.

Shifting focus to feature optimisation, [48] employs feature weighting, prioritising more important features to improve detection. Tested on KDD-99 against DoS, probing, U2R, and R2L attacks, this approach achieves 99.7% accuracy and 94.7% precision. The authors observe that performance varies across datasets and recommend testing in diverse network settings to validate the method's robustness.

Most of the papers discussed in this sub-theme acknowledge the equal importance of data and algorithms. Each paper proposes different methodologies, which demonstrate the absence of a universal solution. Furthermore, each concludes with a candid acknowledgment: a method effective on one dataset may not be applicable to another. Consequently, the shared subsequent step is to test across a broader range of environments.

4.3.3. Feature Selection and Dimensionality Control

Network traffic data contains thousands of features and millions of packets. Running ML on all data is slow and expensive. Many features add little value, making models heavier and harder to interpret. Feature selection helps identify the smallest set of features that reliably detects attacks.

[49] deals with two common problems in intrusion detection: 1) having too many features and 2) the high cost of labelling data. They proposed a semi-supervised framework that integrates a collection of intelligent strategies. First, they remove features that are less useful using information gain and the Fisher score. PCA is then used to reduce the dimensionality. Lastly, they present Tri-LightGBM, an enhanced version of LightGBM that employs stratified sampling to learn from both labelled and unlabelled data. Tests on the UNSW-NB15 and CIC-IDS-2017 datasets, which contain attacks such as backdoors, DoS, fuzzers, worms, and exploits, yielded good results. The multi-strategy feature filtering cut down on false positives by the same amount, while improving accuracy, recall, and precision by about 0.5%. It also made the precision of the minority attack category better by 1% to 2%. The authors acknowledge that dataset imbalance persists as a challenge and recommend that subsequent research explore incremental learning to facilitate progress over time. A recent work [50] combines CNNs and LSTMs with Bayesian optimisation for IoT threat detection. On UNSW-NB15, the model achieves 78.47% binary and 78.36% multiclass accuracy. Still, the authors note challenges with hyperparameter tuning and dataset limitations.

In a related optimisation-focused study, [51] uses Moth Flame Optimisation (MFO) with a decision tree-based Bagging ensemble, achieving an 87.43% detection rate on NSL-KDD with low time overhead. The authors note that scalability limits require further testing in larger environments. Extending the focus to sequence learning, [52] compares RNNs, LSTMs, GRUs, and BERT on the CIC-DDoS2019 dataset. The study finds that sequence-based models effectively capture temporal relations, with RNN

 doi:10.20944/preprints202605.1231.v1

achieving 97.85% accuracy. Notably, BERT underperforms, suggesting that transformers are not always optimal for structured network data.

Several notable patterns emerge from the analysis. Firstly, the efficiency of feature selection is evident. Most studies demonstrate that it is possible to reduce the number of features without compromising accuracy. In some instances, accuracy is even enhanced. Secondly, rare attacks continue to pose significant challenges. Specifically, R2L and U2R attacks remain challenging to detect, even with advanced feature selection techniques. Thirdly, there exists a trade-off between model complexity and performance. The most favourable results are often achieved with the most complex models. Identifying the optimal balance, where the model is sufficiently lightweight for real-time application, remains the primary challenge.

4.4. Theme 4: Deep Neural Architectures for Representation Learning in IDS

This theme focuses on deep learning's primary strength: automatic learning of hierarchical representations from raw or minimally processed data. This theme encompasses the evolution from simple architectures to sophisticated designs that capture spatial, temporal, and relational patterns in network traffic.

4.4.1. Convolution-Centric Intrusion Modeling

CNNs were made for images, but researchers have found clever ways to adapt them for network traffic. By treating packets like pixels and flows like images, CNNs can automatically learn patterns that might be hard to capture with hand-crafted features. The papers in this section show just how far this idea can go.

[53] combines VGG16, VGG19, and Xception CNN architectures with Bayesian optimisation. Tested on UNSW-NB15 and CIC DDoS 2019, it achieves 99.26% accuracy on DDoS and 96.23% on UNSW-NB15, outperforming individual models. The authors acknowledge limitations in zero-day attack detection and suggest future work on detecting unknown traffic. A recent work by [54] assesses traditional ML models (Random Forest, SVM) and deep learning models (ResNet, TabNet, VGGNet) on the CICIDS-2017 dataset for DDoS detection. With an accuracy of 99.96% as opposed to 99.91%, Random Forest performs better than VGGNet. Although TabNet balances accuracy and efficiency, deep learning models take longer to train. Scalability and real-time processing remain a significant challenge.

The effectiveness of convolutional approaches extends beyond general network intrusion detection, as demonstrated in [26], which shows convolutional models' strong performance across network types—from general networks to IoT and medical IoT traffic. Continuing the focus on CNN-based methods, [55] presents a custom CNN architecture for intrusion detection. On the NSL-KDD dataset, it achieves 98.5% accuracy against DoS, U2R, R2L, and probing attacks. The authors suggest transfer learning as a promising direction for addressing unseen attacks, echoing concerns about zero-day threats raised in earlier work. Similarly, leveraging deep learning, [56] implements ResNet-CNN, achieving 98.94% binary and 98.92% multiclass accuracy on NSL-KDD. Individual attack detection exceeds 99%, though the authors note that scalability and adapting to new attack patterns remain significant challenges.

[57] introduced a novel preprocessing technique that converts network traffic to heatmaps for CNN analysis. On the NF-UQ-NIDS-v2 dataset, this approach achieves 93.5% accuracy, with AUCs of 0.965 for DoS, 0.860 for SQL Injection, and 0.910 for benign traffic. Despite these promising results, the authors identify dataset imbalance as a key limitation requiring further attention.

Several key themes emerge from the analysis of these papers. Firstly, CNNs have demonstrated efficacy in intrusion detection tasks. Whether employing pre-existing architectures or custom-designed models, CNNs consistently outperform traditional methods. Secondly, while the reported accuracy rates are often high (i.e., frequently exceeding 98%), the papers candidly acknowledge existing limitations, such as challenges posed by zero-day attacks, novel patterns, and the need for real-time processing. Thirdly, the selection of datasets is crucial. While the NSL-KDD dataset is frequently

 doi:10.20944/preprints202605.1231.v1

utilised, there is a growing trend towards incorporating more recent datasets, such as CIC DDoS 2019 and NF-UQ-NIDS-v2, which is a positive development for the field.

4.4.2. Temporal Sequence Intrusion Modeling

Network traffic is not just a collection of independent events. It is a stream—a sequence of packets that unfolds over time. Attacks rarely happen in isolation; they have rhythm, patterns, and dependencies. That is why RNNs, LSTMs, and GRUs are such natural fits for intrusion detection. They remember. The papers in this section show what happens when you let models capture time.

Moving from comparison to application, [58] develops a self-healing system combining signature and anomaly detection. C5 classifiers achieve 97% true positives with 8% false positives on UNSW-NB15, while LSTM gets 90% detection with 17% false alarms on ADFA-LD. The authors emphasise that reducing false alarms remains a central goal for practical deployment.

Several patterns emerge from the analysis. Firstly, sequence models, including LSTM, GRU, and even basic RNNs, effectively capture attack patterns. Secondly, optimisation techniques, such as the seagull algorithm and the grey wolf optimiser, significantly enhance performance through parameter tuning. Thirdly, the most challenging issues remain unresolved, including rare and unknown attacks and the need to adapt to novel environments.

4.4.3. Attention and Transformer-Based IDS

Transformers changed natural language processing. Now they are starting to change intrusion detection, too. Unlike RNNs, which process data step by step, Transformers can process entire sequences at once and identify which parts matter most. That "attention" mechanism is powerful. The papers in this section are early explorers of what attention can do for network security. For example, [59] builds a bridge between old and new. Their CRNN-SA model combines a CNN, an RNN, and self-attention to capture spatial and temporal patterns. On UNSW-NB15 across nine attack categories, binary classification achieves 90.4% accuracy and 91.3% F1 score. Multiclass shows 89.9% accuracy but 77.5% F1 score. The authors aim to speed up training and testing. Addressing the challenge of model optimisation, [60] combines GRU and MLP with the Improved Seagull Optimisation Algorithm (ISOA) for hyperparameter tuning. On the NSL-KDD dataset, this approach achieves 97.59% accuracy, a 97.94% detection rate, and just 2.01% false alarms, outperforming basic models. However, R2L and U2R attacks remain difficult to detect, highlighting a persistent issue in intrusion detection.

Taking hybridisation a step further, [61] combines CNN, BiLSTM, and self-attention into a single unified architecture. Testing on NSL-KDD, UNSW-NB15, and IoTID20 yields impressive results: 99.93%, 99.70%, and 99.78% accuracy, respectively. However, the authors caution that overfitting concerns persist for real-world applications, echoing the generalisation challenges noted in other complex models.

The common thread among these papers is threefold. Firstly, attention mechanisms have demonstrated significant utility by enabling models to concentrate on pertinent information. Secondly, hybrid architectures have become the standard, with attention mechanisms proving most effective when integrated with CNNs, Recurrent Neural Networks (RNNs), or both. Thirdly, while the quantitative results are noteworthy, the field remains nascent. Each paper concludes with limitations, such as scalability, overfitting, and real-time performance. Although transformers exhibit considerable potential, there remains much to be explored and understood.

4.4.4. Autoencoder-Based Anomaly Detection

Most IDS systems are trained to recognise the characteristics of known attack classes. On the other hand, Autoencoder-based systems use an inverted detection paradigm, modeling the distribution of regular traffic and flagging any deviations as anomalies. When network traffic changes from what was learned to be usual, reconstruction error increases, activating an alert. This method is particularly suited to zero-day and previously unseen attack detection. This is due to the fact that it does not require labelled attack samples during training. Extending autoencoder applications to

 doi:10.20944/preprints202605.1231.v1

mobile environments, [62] addresses Mobile Ad-Hoc Networks (MANETs) using Stacked AE-IDS, which combines an autoencoder and a DNN for DoS attack classification. Results show improved detection, though specific performance numbers are not provided in the study. The authors aim to expand testing to cover different attack types in future work.

Taking a multi-source data approach, [63] combines network traffic and social media data using LSTM and Auto-Encoder ensembles. Tested on NSL-KDD and CIC Truth Seeker 2023, it achieves 90.67% accuracy, 97.44% precision, 85.78% recall, and 91.18% F1 score. The authors note that feature fusion across disparate data sources remains a significant challenge.

What ties these research works together? Firstly, autoencoders are great at anomaly detection—they catch what does not fit. Secondly, they play well with others. Almost every paper here pairs autoencoders with something else: CNNs, LSTMs, optimisers, classifiers. Thirdly, the field is moving toward lighter models that can run at the edge. [31] points the way, and others are starting to follow.

4.5. Theme 5: Trustworthiness—Adversarial Robustness, Zero-Day Detection, and Explainability

This theme addresses the critical requirements for deploying IDS in real-world environments: systems must be trustworthy. This includes robustness against adversaries who actively try to evade detection, the ability to detect novel (zero-day) attacks, and explainability to build trust with human operators.

4.5.1. Adversarially Robust IDS

An underexamined and critical vulnerability of ML-based IDS is exposure to adversarial manipulation. Minimally perturbed inputs (modifications unnoticeable to human analysts yet sufficient to alter model predictions) can bypass even high-performing detection models. This adversarial threat poses a fundamental challenge to operational deployment; if attackers can evade detection simply by targeted perturbations to malicious traffic, the practical value of real-world validated detection rates is substantially diminished. A small but important set of papers takes this problem head-on. Taking a comparative approach, [64] evaluates CNN and MLP on NSL-KDD under adversarial conditions. CNN achieves 92.4% accuracy, outperforming traditional methods, though the authors caution that results depend heavily on parameter selection and dataset characteristics. On the same line, [65] tackles adversarial attacks using a combination of Independent Component Analysis (ICA), RFE, Projected Gradient Descent (PGD), and Pigeon-Inspired Optimisation, alongside Spatial Smoothing. Against JSMA, FGSM, and C&W attacks, the model achieves 99.65% accuracy with just a 1.29% attack success rate, though computational efficiency remains an ongoing issue.

Building on the theme of attention mechanisms, [66] creates ADCEN—an ensemble of DTCN, LSTM, GRU, and attention mechanisms, tuned by an improved Cheetah Optimiser. When targeting adversarial evasion attacks, it achieves 95% accuracy with a 4.9% false-positive rate. The authors acknowledge that a key challenge remains: determining whether the model will handle evolving attack strategies over time.

[67] runs a straightforward experiment, comparing SVC, Naïve Bayes, Logistic Regression, Decision Tree, and XGBoost on KDDcuPaper 1999 against DoS, U2R, R2L, and probing attacks. XGBoost comes out on top: 98.80% accuracy, 98.40% recall, 98.50% precision. While the quantitative data presented are robust, the more significant aspect lies in the authors' omissions. They did not conduct empirical tests on adversarial attacks. Instead, they merely acknowledged the importance of adversarial robustness and proposed DL as a potential avenue for future research.

[68] goes deeper into packet payloads. Their meta-heuristic generative model swaps code units in payloads with functionally equivalent alternatives. The goal is to create adversarial examples that keep the same meaning but fool the classifier. The results are striking. When the test classifier shares the same architecture as the surrogate model, adversarial examples get through 69% of the time. Raw examples? Only 5%. That is a huge jump. It shows just how vulnerable these systems are. But there is a catch. The cyber domain is constrained. You cannot just flip bits randomly—traffic still has to make

 doi:10.20944/preprints202605.1231.v1

sense. That limits how well adversarial examples transfer between different models. The authors want future work to focus on robust learning, building systems that are harder to fool in the first place.

This analysis reveals key findings. The field remains underexplored, with only two studies addressing adversarial robustness despite the threat posed by such attacks. Empirical evaluation shows detection can be easily circumvented, with a 69% penetration rate. A gap exists between problem recognition and solution development, as most literature assumes benign conditions rather than real-world scenarios. Adversarial robustness is a fundamental concern that requires greater scholarly attention to develop effective IDS.

4.5.2. Zero-Day and Anomaly-Centric Detection

Signature-based detection works well against known threat profiles but is inherently limited in detecting novel attacks that lack signatures. Zero-day vulnerabilities, being unrecorded at the time of exploitation, therefore represent a fundamental gap in signature-dependent approaches. Anomaly-based detection addresses this problem by creating a baseline of normal network behaviour and identifying statistically significant deviations. This enables the detection of threats that have not been previously discovered.

The papers in this section try to push that idea further. Under this theme is the work of [69], which combines a CNN with a Deep Watershed Autoencoder (CNN-DWA). The autoencoder spots anomalies, while the CNN classifies them. On the KDD CUP 1999 dataset against DoS, U2R, R2L, and probing attacks, it achieves 98.05% accuracy, beating a plain CNN by 3.5%. Zero-day attacks remain challenging. Continuing the focus on autoencoder-based methods, [70] presents a system that uses a Stacked Autoencoder for detection, the Grey Wolf Optimiser for feature selection, and Random Forest or LightGBM for classification. On UNSW-NB15, it achieves 90.94% accuracy, and on CIC-IDS-2017, 99.67%. The authors emphasise adaptability and real-time performance as key priorities for deployment.

Within the same theme is the work of [71], which compares Decision Tree, KNN, and Logistic Regression on the UNSW-NB15 dataset. Decision Tree achieves 98% accuracy against zero-day, DoS, and persistent threats. Class imbalance remains an issue, with ensemble methods suggested as solutions. A recent work by [72] focuses on DoS attacks in IoT. The work uses Random Boruta Selector, Relief, and the Pearson correlation coefficient for feature selection. It uses stacked learning to sort them, achieving 96.5% accuracy and 96% F1-score on the CICDDoS-2019 dataset. The limitation of the study is that it can not handle larger datasets. Taking a different perspective on detection challenges, [73] addresses open-set scenarios using BiGRU with prototype learning and Extreme Value Theory. Tested on CICIDS2017 and pipeline data, it achieves 99.72% accuracy for known classes and an impressive 99.91% detection rate for unknown classes, though the authors note that performance varies with the degree of dataset openness.

Addressing the challenge of identifying novel threats, [74] uses active learning to identify new attacks with minimal labeled examples. The system combines signatures with incremental class addition. Tested on CICIDS-2017 across various attack types, it achieves 0.894 accuracy and 0.723 balanced accuracy, remaining near the baseline performance. The authors note that performance initially drops when new attacks are introduced, highlighting a key limitation of incremental learning approaches.

What pattern does emerge? Zero-day detection is hard. Every paper here makes progress, but none claim to have solved it. Adaptation is key. Whether through continuous learning, active learning, or optimisation, models need to keep evolving.

4.5.3. Explainable Artificial Intelligence (XAI) IDS

A fundamental limitation of many ML-based IDS is their black-box nature. They flag an alert, but no one knows why. In critical infrastructure, that is not good enough. Security analysts need to understand what triggered the alarm. Was it a real threat? A false positive? Something in between? Without explanations, trust erodes. And in regulated industries, compliance often demands answers.

 doi:10.20944/preprints202605.1231.v1

XAI is the attempt to open the black box. The papers in this section are rare examples of researchers taking this seriously.

[75] evaluates four explanation methods (Permutation Importance, SHAP, LIME, CIU) on IDS models to provide global and local explanations. Tests on NSL-KDD and Kaggle datasets show Random Forest and XGBoost achieving 70-75% accuracy using the top 15 XAI-selected features. Key issues identified include computational expense and Permutation Importance's tendency to overestimate the importance of correlated features.

Extending XAI to DL models, [76] develops BiLSTM-XAI, which combines a Bidirectional LSTM with SHAP, LIME, and Krill Herd optimisation. Testing on Honeypot and NSL-KDD datasets achieves 98.2% accuracy for detecting Industry 4.0 threats. While the explanations help clarify LSTM operations, adversarial attacks remain a significant challenge, prompting the authors to suggest future work on hybrid metaheuristic approaches to enhance robustness.

There are a few important things to note about the current state of research. To begin with, there is little research on XAI in IDS, with only two papers addressing this area. This lack of information is worrying because black-box models are hard to trust and debug. Second, existing studies show that explanations can help people understand things better without affecting performance. Thirdly, there are still big problems to solve, such as high computational costs, correlated features, and adversarial robustness. For IDS to be effectively deployed in critical systems, explainability must be integrated into the design process from the outset, rather than being considered retrospectively.

5. Discussion

Having presented the descriptive and thematic analyses, this section synthesises the key findings, discusses emerging patterns, and identifies ongoing challenges that shape the current landscape of ML-based IDS research. Table 3 provides the full thematic classification of all 125 reviewed papers. It details each study's year, algorithm, dataset, and attack vector.

5.1. Summary of Findings

Figure 6 and Table 4 reveal the growth directions of the five themes. Theme 1 as discussed in Section 4.1 continues its growth, increasing from 5 papers in 2022 to 10 in 2025, showing the field's ongoing interest in integrating multiple models to improve performance. Theme 5 as described in Section 4.5 is emerging as a new focus area, growing from 1 to 5 papers over the same period, yet this remains a small proportion of the corpus. Theme 4 demonstrated in Section 4.4 exhibits consistent momentum, reaching 9 papers in 2024 before slightly declining to 8 in 2025. Overall, the total number of annual publications increased from 19 in 2022 to 42 in 2025, demonstrating sustained research interest in ML-based IDS.

The algorithmic terrain reveals a pluralistic approach rather than an entire shift to DL. Researchers frequently integrate both approaches. The overlap is evident in hybrid CNN-LSTM architectures as discussed before. This finding aligns with the domain's mature understanding that intrusion detection requires both spatial (i.e., packet content) and temporal (i.e., sequential) analysis. Transformers are notably under-explored, with only 8 published papers, presenting a substantial research opportunity due to their proven ability to capture long-range associations in many sequence modelling domains.

The selection of datasets remains a significant concern. As shown in Table 2, the NSL-KDD dataset (established in 2009 and reflecting patterns from the late 1990s) has accounted for 19.2% of dataset utilisation. This continued dependency on legacy datasets indicates that the field may be optimised for historical benchmarks rather than modern attack vectors. This likely clarifies the narrow attack surface observed in the literature, where volumetric attacks (DDoS/DoS) overwhelm research, while web attacks, ransomware, and advanced persistent threats remain significantly understudied. Yet to mention zero-day detection.

 doi:10.20944/preprints202605.1231.v1

Table 3. Thematic Classification of 125 Reviewed Papers with Key Details.

Theme 1: Ensemble & Hybrid Learning Pipelines (30 papers)				
#	**Paper ID**	**Year**	**Key Algorithms & Datasets**	**Attacks Vector**
1	[42]	2025	Uses class-imbalance handling on NSL-KDD.	DoS, Root-to-Local (R2L), User-to-Root (U2R), probe attacks
2	[54]	2025	Uses ResNet on CICIDS-2017.	DDoS
3	[11]	2022	Compares ML classifiers on NSL-KDD.	DoS-SlowHTTPTest, DoS-Hulk, DoS-GoldenEye, DoS-Slowloris, BruteForce-Web, BruteForce-XSS, SQL Injection, FTP-BruteForce, SSH-BruteForce, DDOS-LOIC-UDP, DDOS-HOIC
4	[49]	2022	Uses PCA on UNSW-NB15.	Backdoors, DoS, Analysis, Fuzzers, Worms, Reconnaissance, Shellcode, Exploits
5	[36]	2024	Uses LSTM on car hacking dataset.	DoS, fuzzy attacks, spoofing RPM attacks
6	[22]	2025	Uses Random Forest on CICDS2018.	unknown
7	[13]	2023	SDN with RF+SVM.	DDoS
8	[72]	2025	Uses Stacked Learning Classifiers on CICDDOS-2019.	DoS
9	[34]	2022	Uses bagging	Slow-Read DDoS, data exfiltration using DNS tunneling
10	[35]	2025	Ensembles ANN+tree models on NSL-KDD.	unknown
11	[19]	2025	Uses Random Forest on New Dataset.	unknown
12	[77]	2025	Tree/boosting models on CICIDS2017.	unknown
13	[78]	2024	RF/DT on IoT botnet dataset (CTU-13).	unknown
14	[79]	2025	Socioeconomic data incorporation.	DoS, probing, U2R, remote-to-local (R2L)
15	[80]	2025	Optimises CNN/LSTM pipeline on CICIDS2017.	unknown
16	[75]	2022	Uses XGBoost with SHAP on NSL-KDD.	DoS attack variants
17	[81]	2025	Energy-efficient IDS (RF) for IoT on CICIDS2017.	unknown
18	[82]	2025	Incremental learning for streaming IDS on NSL-KDD.	DoS, R2L, U2R, Probe
19	[83]	2022	RNN for skeleton-based action recognition.	Fast Gradient Sign Method (FGSM), Jacobian-based Saliency Map Approach (JSMA), DeepFool, Carlini and Wagner (CW) attacks
20	[84]	2023	Hybrid SVM model on NSL-KDD.	Unknown
21	[85]	2024	Decision tree for IoT (i.e. smart city) on NSL-KDD.	Unknown
22	[86]	2025	ANN/SVM on NSL-KDD.	Zero-day attack detection
23	[87]	2025	Random Forest baseline on NSL-KDD.	DoS, R2L, U2R, probing attacks
24	[88]	2025	Studies feature preprocessing on NSL-KDD.	Brute Force, DoS, PortScan
25	[89]	2022	Random Forest vs. SVM on KDD-99.	DoS, U2R, R2L, probe attacks
26	[90]	2025	Real-time CNN-LSTM-XGBoost IDS on CICIDS2017.	DoS, Port Scan, Brute Force, Web Attack, Bot, Infiltration, DDoS, Heartbleed
27	[91]	2024	RF/DT ensemble on CICIDS2017.	FTP Patator, SSH Patator, DoS, BruteForce, XSS, SQL Injection
28	[92]	2025	CNN+LSTM for diverse IDS scenarios. No Datasets	Unknown
29	[93]	2023	Uses DNN on KDD-99.	DoS, eavesdropping, ransomware attacks
30	[94]	2025	ML for vehicle movement (ITS).	DoS, Probing, U2R, R2L
31	[95]	2023	RF with feature selection for cloud IDS on NSL-KDD.	Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, Worms
Theme 2: Context-Specific IDS Design (34 papers)				
#	**Paper ID**	**Year**	**Key Algorithms & Datasets**	**Attacks Vector**
32	[26]	2024	Uses CNN on CICIOT2023.	DDoS, DoS, Mirai, web-based, reconnaissance
33	[27]	2023	Uses LSTM on CICIDS2017.	DDoS, PortScan, Botnet, Infiltration

 doi:10.20944/preprints202605.1231.v1

#	Paper ID	Year	Key Algorithms & Datasets	Attack Vector
34	[28]	2025	Uses ANN on CIC IoT 2022.	unknown
35	[29]	2025	Uses ANN on NSL-KDD.	DoS, Probe
36	[30]	2023	Uses IoT IDS setting on Contiki Cooja simulator.	Sinkhole Attacks
37	[50]	2025	CNN-LSTM with PCA preprocessing.	DoS, Generic, Backdoor, Shellcode, Exploits, Reconnaissance, Fuzzers, Worms
38	[71]	2024	ML, K-NN, and Classification on UNSW-NB15.	Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, Worms
39	[37]	2025	Uses LSTM on NSL-KDD.	unknown
40	[38]	2025	Uses MASNet.	Unknown
41	[39]	2025	Uses SDN/cloud-context IDS on CSE-CIC-IDS2018.	hypervisor attacks, user-to-root attacks, insider attacks, port scanning, backdoor channel attacks, DoS attacks, flooding attacks, Economic Denial of Sustainability (EDoS) attacks
42	[40]	2023	Uses Deep Learning on KDD-99.	Unknown
43	[33]	2025	Lightweight IDS for IoT networks.	unknown
44	[16]	2024	Uses Random Forest on NSL-KDD.	Unknown
45	[96]	2023	Uses ANN on MQTT-IDS-2020.	Unknown
46	[97]	2023	ANN for IoT device IDS on CICIDS2017.	Heartbleed, botnet, SSH brute-forcing, web login brute-forcing, DoS, DDoS, SQL injection, infiltration, Cross-Site Scripting (XSS)
47	[98]	2024	ML for sensor network IDS.	Unknown
48	[90]	2025	Real-time CNN-LSTM-XGBoost IDS on CICIDS2017.	DoS, Port Scan, Brute Force, Web Attack, Bot, Infiltration, DDoS, Heartbleed
49	[99]	2024	Multi-stack deep model for cloud IDS.	Unknown
50	[100]	2025	Uses Genetic Algorithm.	Unknown
51	[101]	2024	Uses deep model on KDD-99.	DoS, Probe, R2L, U2R, network traffic attacks
52	[102]	2024	Uses SMOTE on UNSW-NB15.	Unknown
53	[25]	2023	Uses Random Forest on NSL-KDD.	DoS, Probe, U2R, R2L
54	[103]	2025	Uses ANN/DNN on UNSW-NB15.	unknown
55	[104]	2024	Uses CNN on NSL-KDD.	unknown
56	[15]	2024	Uses deep learning and ensemble methods on NSL-KDD.	DoS, R2L, U2R, Probe
57	[105]	2023	Metaheuristic-optimised RNN on NSL-KDD.	Unknown
58	[106]	2022	Combines multiple datasets (i.e., NSL-KDD, etc.) with adaptive learning.	unknown
59	[12]	2022	Hybrid CNN-LSTM-GAN model on NSL-KDD.	Unknown
60	[107]	2025	Multi-level ensemble on NSL-KDD.	Unknown
61	[108]	2023	Ensembles ML for high-speed traffic (KDD-99).	DDoS, DoS, Brute Force, SQL Injection, Malware, Phishing
62	[109]	2024	Classical ML classifiers on NSL-KDD.	Unknown
63	[110]	2025	Deep ensemble improves minority detection on KDD-99.	Unknown
64	[53]	2024	Uses VGG on CICDDOS2019.	DDoS, exploits, reconnaissance
65	[55]	2025	Uses CNN on combined datasets.	Unknown

Theme 3: Data-Centric Engineering (20 papers)

#	Paper ID	Year	Key Algorithms & Datasets	Attacks Vector
66	[44]	2025	Uses SMOTE on CIC-IDS2017.	Dos Hulk, PortScan, DDos, Dos GoldenEye, FTP-Patator, SSH-Patator, Dos slowloris, Dos Slowhttptest, Bot, Web Attack Brute Force, Web Attack XSS, Infiltration, Web Attack Sql Injection, Heartbleed
67	[12]	2022	Hybrid CNN-LSTM-GAN model on NSL-KDD.	unknown

 doi:10.20944/preprints202605.1231.v1

#	Paper ID	Year	Key Algorithms & Datasets	Attack Vector
68	[111]	2025	Trains on real-world dataset (CICIDS2017).	Unknown
69	[45]	2024	Oversampling for imbalanced NSL-KDD.	Unknown
70	[46]	2025	Uses ADASYN on UNSW-NB15.	unknown
71	[14]	2023	Uses fuzzy subset linked model.	unknown
72	[47]	2025	Uses GAN on NSL-KDD.	unknown
73	[48]	2025	Uses ensemble tree on KDD-99.	DoS, Probe, U2R, R2L
74	[25]	2023	Uses Random Forest on NSL-KDD.	DoS, Probe, U2R, R2L
75	[15]	2024	Uses deep learning and ensemble methods on NSL-KDD.	DoS, R2L, U2R, Probe
76	[41]	2023	Uses class-imbalance handling on UNSW-NB15.	unknown
77	[51]	2022	Uses feature selection on NSL-KDD.	unknown
78	[65]	2025	Uses FGSM.	Jacobian Saliency Map Attacks (JSMA), Fast Gradient Sign Method (FGSM), Carlini and Wagner (C&W)
79	[112]	2023	Uses LSTM.	unknown
80	[113]	2023	Uses adversarial robustness on KDD-99.	unknown
81	[114]	2024	Uses LSTM on CICIDS2017.	DoS, DDoS, web attacks
82	[115]	2024	Uses tree ensemble on CIC-IDS2017.	DDoS, botnets, DNS over HTTPS (DoH) threats
83	[116]	2025	Uses CNN + SVM.	DoS, Probe, R2L, U2R
84	[76]	2023	Metaheuristic-optimised LSTM on NSL-KDD.	unknown
85	[117]	2025	Class imbalance analysis on CIC-Bell-IDS2017.	unknown
86	[118]	2025	Lightweight IDS for IoT devices.	unknown

Theme 4: Deep Neural Architectures (31 papers)

#	Paper ID	Year	Key Algorithms & Datasets	Attacks Vector
87	[56]	2025	Uses CNN on NSL-KDD.	unknown
88	[64]	2025	Uses adversarial robustness on NSL-KDD.	unknown
89	[57]	2024	Uses CNN on heatmap features (NF-UQ-NIDSv2).	DoS, SQL Injection
90	[17]	2025	Uses CNN + SVM on NSL-KDD.	unknown
91	[52]	2025	Uses feature selection/dimensionality reduction on CIC-DDoS2019.	DDoS
92	[58]	2024	Uses LSTM on UNSW-NB15.	unknown
93	[60]	2024	LSTM with attention on NSL-KDD.	unknown
94	[73]	2024	GRU-based incremental learning for ICS.	DDoS, DoS GoldenEye, FTP-patator, SSH-patayor, DoS slowloris, DoS slowhttptest, Web attack, Bot, Infiltration, Heartbleed
95	[23]	2024	GRU-based ICS anomaly detection.	unknown
96	[59]	2023	Uses Transformer on UNSW-NB15.	unknown
97	[66]	2025	Uses Attention.	adversarial evasion assaults
98	[18]	2025	CNN-LSTM with XGBoost ensemble on NSL-KDD.	unknown
99	[61]	2025	CNN-LSTM-Transformer model on NSL-KDD.	unknown
100	[69]	2023	Uses zero-day detection on KDD-99.	DoS, U2R, R2L, Probing
101	[70]	2023	Uses zero-day detection on CIC-IDS-2017.	zero-day attack detection
102	[62]	2023	Stacked autoencoder for MANET intrusion detection.	DoS attacks
103	[63]	2025	Fuses social media data into IDS.	click-baits, phishing techniques

 doi:10.20944/preprints202605.1231.v1

#	Paper ID	Year	Key Algorithms & Datasets	Attack Vector
104	[31]	2024	Lightweight CNN+LSTM on IoT data.	DDoS, port scanning, brute force attacks, DoS attacks, botnet traffic, Mirai botnet
105	[119]	2025	Naive Bayes baseline on NSL-KDD.	unknown
106	[120]	2024	Tree ensembles for generalizability on NSL-KDD.	unknown
107	[74]	2024	Incremental adaptive NN on CICIDS2017.	Botnet, Brute Force, DoS, Heartbleed, Infiltration, DDoS, Web Attacks
108	[21]	2024	CNN-LSTM ensemble for IDS on CICIDS2017.	zero-day attacks, changing behaviours of benign users/applications
109	[43]	2025	Optimised ML for minority classes on UNSW-NB15.	DoS, Exploits, Fuzzers, Worms
110	[121]	2025	CNN+RF high-precision IDS on CICIDS2017.	unknown
111	[122]	2025	CNN+GRU ensemble on KDD-99.	DoS, Probe, R2L, U2R
112	[123]	2024	CNN+attention with limited data on NSL-KDD.	DoS, DDoS, Web Attacks
113	[124]	2022	Transfer learning (CNN+LSTM) on NSL-KDD.	unknown
114	[125]	2024	Constructs knowledge graph from cyber data.	unknown
115	[126]	2025	Multi-dataset evaluation for IDS.	BruteForce FTP-Patator, SSH-Patator, PortScan, DDoS LOIT, Botnet ARES, Infiltration – Dropbox Download, Meta exploit
116	[67]	2025	Uses XGBoost on KDD-99.	DoS, U2R, R2L, probing
117	[68]	2023	Uses adversarial robustness on Deep learning.	adversarial ML methods
Theme 5: Trustworthiness (10 papers)				
#	Paper ID	Year	Key Algorithms & Datasets	Attacks Vector
118	[21]	2024	CNN-LSTM ensemble for IDS on CICIDS2017.	zero-day attacks, changing behaviors of benign users/applications
119	[74]	2024	Incremental adaptive NN on CICIDS2017.	Botnet, Brute Force, DoS, Heartbleed, Infiltration, DDoS, Web Attacks
120	[43]	2025	Optimised ML for minority classes on UNSW-NB15.	DoS, Exploits, Fuzzers, Worms
121	[20]	2023	Butterfly-optimised deep model on NSL-KDD.	DoS, probe, U2R, R2L
122	[75]	2022	Uses XGBoost with SHAP on NSL-KDD.	DoS attack variants
123	[76]	2023	Metaheuristic-optimised LSTM on NSL-KDD.	unknown
124	[127]	2024	CNN+LSTM pipeline on NSL-KDD.	SQL Injection, Cross Site Scripting (XSS), Brute Force
125	[128]	2025	Optimises malware classification features.	Trojan, Spyware, Ransomware

 doi:10.20944/preprints202605.1231.v1

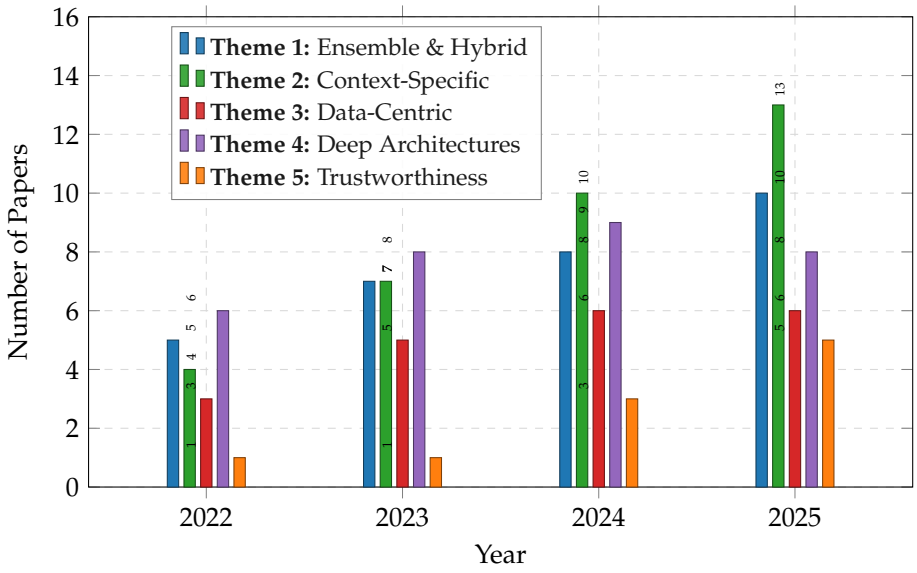

Figure 6. Distribution of Papers by Theme and Year.

Table 4. Numerical distribution of papers by theme and year.

Theme	2022	2023	2024	2025	Total
Theme 1: Ensemble & Hybrid	5	7	8	10	30
Theme 2: Context-Specific	4	7	10	13	34
Theme 3: Data-Centric	3	5	6	6	20
Theme 4: Deep Architectures	6	8	9	8	31
Theme 5: Trustworthiness	1	1	3	5	10
Total	**19**	**28**	**36**	**42**	**125**

5.2. Identified Research Gaps

1. **Limited Threat Vector Coverage:** Most studies evaluate IDS models against a limited number of attack types. For example, only [108] comprehensively addresses six attack vectors (i.e., brute force, DoS, DDoS, malware, phishing, and SQL injection). The majority of papers focus narrowly on volumetric attacks (DDoS/DoS), such as those by [13,38,52–54]. Moreover, many papers do not even specify the type of attack they target, such as the work by [39,42,48,129,130]. Thus, the models are unattainable for evaluating their relevance to real-world threats. This limited threat-vector coverage neglects significant attack categories, including online attacks, ransomware, web attacks, APTs, etc.
2. **Adversarial Robustness:** A critical yet insufficiently examined issue is that ML-based IDS can be bypassed by carefully crafted adversarial samples. An attacker could subtly modify malicious traffic to bypass detection while maintaining its dangerous functionality. Given the severity of this threat, merely five works explicitly address adversarial robustness ([52,53,66–68]). The vast majority of the researched papers assume benign testing conditions and do not evaluate their models against adversarial attacks (e.g., [17,52,53]). This creates a dangerous gap between experimental claims and real-world resilience.
3. **Zero-day Detection:** Anomaly-based approaches theoretically facilitate zero-day detection, but practical validation remains limited. The majority of proposals employ semi-supervised methods to identify known attack patterns, rather than truly novel threats ([63,69,70]). Some papers address concept drift, such as [21,74], but none validate their model against truly novel attacks in real-world settings. A primary contributing factor is that most studies train and evaluate on a single dataset from a similar context, failing to replicate the distribution shifts characteristic of real-world zero-day scenarios.

 doi:10.20944/preprints202605.1231.v1

4. **Explainable AI (XAI):** Security analysts need to understand why an alert was triggered, yet the literature neglects interpretability. Only two papers integrate XAI into IDS [75,76]. The vast majority of DL papers, such as [17,53,59], employ black-box models without any explanation capabilities. The absence of transparency hinders practical implementation in security operations centres, where explainable decisions are crucial for trust and compliance.

To summarise, less than 2% of reviewed papers incorporate XAI techniques, only 4% focus on adversarial robustness testing, and none validate their models in real-world environments. This gap between laboratory performance and the operational reality is perhaps the most significant finding of this review, suggesting that claims of "state-of-the-art" performance may not translate to practical effectiveness in live network environments.

6. Answers to Research Questions

6.1. RQ1: What Machine Learning (ML) and Deep Learning (DL) Algorithms Are Most Commonly Employed in Intrusion Detection System Research?

The most commonly employed algorithms are CNNs, LSTMs, and Random Forests, often used in hybrid configurations that combine their complementary strengths. Ensemble methods (i.e., particularly tree-based) remain highly competitive with DL approaches.

The analysis reveals a clear hierarchy of algorithmic prevalence in IDS research. As seen in Figure 5, CNNs are used for spatial feature extraction in 35 papers, while LSTM networks are the primary choice for temporal modelling, appearing in 34 papers. The synergy between these architectures is evident in the proposed hybrid CNN-LSTM models, as demonstrated in Section 4.1.2. Turning to classical and ensemble methods, Random Forest remains exceptionally prevalent, appearing in 30 of the reviewed studies, a testament to its robust performance and interpretability (see Subsection 4.1.1).

Beyond DL, gradient-boosting methods such as XGBoost appear in 9 studies, demonstrating that tree-based ensembles remain highly competitive, as discussed in Subsection 4.1.1. Finally, SVM appears in 14 papers, often integrated into ensemble or hybrid models.

6.2. RQ2: What Attack Types and Network Environments Are Addressed by Current ML-Based IDS Proposals, and Where Are the Coverage Gaps?

DDoS/DoS attacks dominate the literature, while IoT and cloud environments are the fastest-growing contexts. Critical gaps exist in web attacks, zero-day detection, and comprehensive multi-attack vector coverage.

The distribution of attack types and network environments in the literature is highly uneven. Volumetric attacks (DDoS and DoS) are the primary focus of the reviewed studies, as seen in Table 3. This is likely attributable to the widespread use of legacy datasets such as NSL-KDD, which predominantly contain volumetric attacks and lack modern threat vectors. At the same time, it reflects the persistent real-world prominence of these threats, with sequence-based models (i.e., LSTM and GRU) proving particularly effective at capturing their temporal patterns (as detailed in Theme 2, Section 4.2).

In terms of deployment environments, the surge in IoT research is driven by the need for lightweight, resource-constrained models. Cloud and SDN environments have also attracted increasing attention. Despite these areas of focus, critical coverage gaps persist. The vast majority of studies evaluate models against only one or two attack types. An exception is the work of [108], whose attack vector covers six or more attacks. Web-based attacks appear in a few papers, which is a concerning gap given their real-world prevalence. Zero-day detection is also widely overlooked, and sophisticated attacks such as R2L and U2R consistently yield lower detection rates due to class imbalance. This uneven landscape suggests that the field must broaden its focus to address the full spectrum of real-world threats.

 doi:10.20944/preprints202605.1231.v1

6.3. RQ3: What Methodological Challenges Remain Unaddressed in ML-Based IDS Research?

A short answer would be that the most critical unaddressed challenges are adversarial robustness, real-world validation, and explainability. Imbalance handling and feature selection are relatively well-addressed.

Despite significant progress in model performance, several fundamental methodological challenges remain largely unaddressed. The most notable gap is in adversarial robustness, with only five studies addressing these carefully crafted attacks (i.e. [64–66,68,113]). Even more concerning is the complete absence of real-world validation. The study reveals that no papers reported production deployments, which limits confidence in operational conditions. Explainability and interpretability are similarly largely neglected, with only two papers (i.e., [75,76]) attempting to open the black box. Zero-day detection, while attempted in five studies, remains in its infancy with limited empirical validation of generalisation. Cross-domain generalisation is another issue, as the ability of models trained on one dataset to perform well on others is largely overlooked. This raises serious concerns about robustness across different network environments.

6.4. RQ4: What Are the Emerging Trends in ML-Based IDS Research, and What Critical Gaps Should Guide Future Investigations?

We identified some emerging trends, including context-specific IDS (IoT/cloud), attention/transformer architectures, and research on trustworthiness. Critical future directions are adversarial robustness, XAI, and real-world deployment.

As seen in Figure 4, the trajectory of ML-based IDS research reveals several clear emerging trends. Context-specific design for IoT and cloud environments has grown rapidly, expanding from 4 papers in 2022 to 13 in 2025. Research on trustworthiness grew from 1 paper in 2022 to 5 in 2025. Attention mechanisms and transformer architectures (i.e., deep architectures) seem consistent across years, while general DL research has plateaued around 8 papers annually since 2024. This may indicate the field has matured towards incremental improvements, rather than fundamental breakthroughs. Ensemble methods have grown to ten papers in 2025, confirming their enduring relevance as reliable, interpretable alternatives.

Given those trends, we suggest that the primary focus for future work must be on the trustworthiness triad:

1. adversarial robustness to prevent active evasion,
2. XAI to build operator trust and enable debugging, and
3. real-world validation to bridge the persistent gap between laboratory performance and operational deployment.

Secondary priorities include advancing zero-day detection capabilities and improving cross-domain generalisation. Together, these directions chart a course for IDS research to move beyond benchmark optimisation toward robust, interpretable, and deployable systems.

7. Conclusion and Future Research Directions

This Systematic Literature Review (SLR) analyses Machine Learning-based Intrusion Detection Systems (ML-based IDS) by integrating 125 peer-reviewed papers published between 2022 and 2025. The review examined publication trends, methodological practices, dataset usage, and the prevalence of algorithms. Publications are growing by 30.2% per year, yet the vast majority evaluate models on legacy benchmark datasets rather than on real-world validation data.

Our five-theme taxonomy organises the literature into (1) ensemble/hybrid pipelines, (2) context-specific designs (IoT, cloud, SDN), (3) data-centric engineering, (4) deep neural architectures, and (5) trustworthiness. Random Forest, CNN, and LSTM remain among the most common algorithms, with growing emphasis on resource-limited environments. Nonetheless, considerable deficiencies persist, as most research focuses on DDoS/DoS detection, while adversarial robustness and XAI remain severely underexplored, and no studies validate models in real-world environments.

 doi:10.20944/preprints202605.1231.v1

This review highlights these gaps and calls for urgent action to translate ML-based IDS research into reliable, practical defenses.

Based on the identified gaps, we propose a prioritised research plan organised into three levels:

Level 1 (Highest Priority): Trustworthiness

- **Adversarial robustness:** Developing models that are resistant to evasion attacks through adversarial training and robust feature engineering, supported by standardised robustness benchmarks.
- **Explainable AI (XAI):** Integrating XAI techniques into IDS architectures from the design phase to provide analysts with clear, actionable explanations while balancing computational costs.
- **Real-world validation:** Transitioning from static CSV files to live network environments by creating industry testbeds to evaluate performance under realistic conditions and evolving attacks.

Level 2 (High Priority): Expanding Threat Coverage

- **Comprehensive Threat Coverage (Beyond DDoS):** Expand beyond volumetric attacks (DoS/DDoS) to include web attacks, ransomware, and Advanced Persistent Threats (APT).
- **Zero-Day and Anomaly Detection:** Advance zero-day detection via self-supervised learning and multimodal data integration.
- **Cross-Domain Generalisation:** Improve cross-domain generalisation using domain adaptation techniques.

Level 3 (Foundational Practices):

- **Dataset modernisation:** Replace legacy datasets with modern, diverse benchmarks reflecting current network traffic and cyberattacks.
- **Lightweight models:** Develop lightweight models for IoT and edge devices through model compression and efficient architectures.
- **Hybrid Architectures:** Explore using meta-learning and ensemble methods to fuse multiple data sources for resilient detection.

Addressing these priorities will shift ML-based IDS from a focus on benchmark optimisation to a domain focused on providing robust, interpretable, and deployable defenses against real-world cyber threats. Without these shifts, the growing gap between reported 'state-of-the-art' performance and operational reality will persist, leaving vital infrastructure vulnerable to attacks that academic research benchmarks do not capture.

Author Contributions: Conceptualisation: Mahmoud H. Qutqut, and Ali Ahmed; methodology: Ali Ahmed, and Mahmoud H. Qutqut; validation: Mahmoud H. Qutqut, Ali Ahmed, Ramy Mostafa, and Noha Ragab; formal analysis: Ali Ahmed, Mahmoud H. Qutqut, Ramy Mostafa, and Noha Ragab; investigation: Ali Ahmed, and Ramy Mostafa; resources: Mahmoud H. Qutqut and Noha Ragab; data curation: Ramy Mostafa, Mahmoud H. Qutqut, and Ali Ahmed; writing: Ali Ahmed, Mahmoud H. Qutqut, Ramy Mostafa, and Noha Ragab; visualisation: Ali Ahmed and Ramy Mostafa; project administration: Ali Ahmed and Mahmoud H. Qutqut. All authors have read and agreed to the published version of the manuscript.

Funding: The APC was funded by the Gulf University for Science & Technology. The Grant Number is 187 and was awarded in the academic year 2025–2026.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: No new data were created or analysed in this study. All data supporting the findings of this work are available within the published articles cited in the manuscript.

Acknowledgments: During the preparation of this manuscript/study, the author(s) used DeepSeek [3] for the purposes of verifying the consistency of the manually identified themes. The authors have reviewed and edited the output and take full responsibility for the content of this publication.

[3] https://chat.deepseek.com, last accessed 18 April 2026

 doi:10.20944/preprints202605.1231.v1

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Ali, T.; Al-Khalidi, M.; Al-Zaidi, R. Information security risk assessment methods in cloud computing: Comprehensive review. *Journal of Computer Information Systems* **2026**, *66*, 123–150. https://doi.org/10.1080/08874417.2024.2329985.
2. Rahman, M.; Alam, S.; Gupta, K.; George, R.; Siddique, S.; Kobayashi, K., Intrusion Detection Systems (IDS) in ICS: Supervisory Frameworks, Signature Versus Anomaly-Based Detection, and Architectural Design. In *Securing Industrial Control Systems: Advanced Strategies and Technologies*; Springer, 2026; pp. 427–463. https://doi.org/10.1007/978-3-032-03018-4_15.
3. Alshaikh Qasem, A.; Qutqut, M.H.; Alhaj, F.; Kitana, A. SRFE: A stepwise recursive feature elimination approach for network intrusion detection systems. *Peer-to-Peer Networking and Applications* **2024**, *17*, 3634–3649. https://doi.org/10.1007/s12083-024-01763-2.
4. Maghanaki, M.; Keramati, S.; Chen, F.F.; Shahin, M. Systematic Evaluation of Machine Learning and Deep Learning Models for IoT Malware Detection Across Ransomware, Rootkit, Spyware, Trojan, Botnet, Worm, Virus, and Keylogger. *Sensors* **2026**, *26*, 1750. https://doi.org/10.3390/s26061750.
5. Issa, M.; Aljanabi, M.; Muhialdeen, H. Systematic literature review on intrusion detection systems: Research trends, algorithms, methods, datasets, and limitations. *Journal of Intelligent Systems* **2024**, *33*. https://doi.org/10.1515/jisys-2023-0248.
6. Satilmiş, H.; Akleylek, S.; Tok, Z.Y. A systematic literature review on host-based intrusion detection systems. *IEEE Access* **2024**, *12*, 27237–27266. https://doi.org/10.1109/ACCESS.2024.3367004.
7. Guntoro, G.; Lisnawita, L.; Costaner, L. Review of Machine Learning Algorithm for Intrusion Detection System. *ComniTech: Journal of Computational Intelligence and Informatics* **2024**, *1*, 26–37.
8. Janati, M.; Messaoudi, F. Intrusion detection system-based network behavior analysis: A systemic literature review. *International Journal of Advanced Computer Science and Applications* **2025**, *16*, 793–802. https://doi.org/10.14569/IJACSA.2025.0160378.
9. Page, M.; McKenzie, J.; Bossuyt, P.; Boutron, I.; Hoffmann, T.; Mulrow, C.; Shamseer, L.; Tetzlaff, J.; Akl, E.; Brennan, S.; et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ (Clinical research education)* **2021**, *327*, n71. https://doi.org/10.1136/bmj.n71.
10. Gartner, Inc.. Gartner Forecasts Information Security Spending in India to Total $3.4 Billion in 2026, 2026. Last accessed: 2026-03-18.
11. Ilyas, M.; Alharbi, S. Machine learning approaches to network intrusion detection for contemporary internet traffic. *Computing* **2022**, *104*, 1061–1076. https://doi.org/10.1007/s00607-021-01050-5.
12. Cui, J.; Zong, L.; Xie, J.; Tang, M. A novel multi-module integrated intrusion detection system for high-dimensional imbalanced data. *Applied Intelligence* **2022**, *53*, 272–288. https://doi.org/10.1007/s10489-022-03361-2.
13. Singh, A.; Kaur, H.; Kaur, N. A novel DDoS detection and mitigation technique using hybrid machine learning model and redirect illegitimate traffic in SDN network. *Cluster Computing* **2023**, *27*, 3537–3557. https://doi.org/10.1007/s10586-023-04152-1.
14. Madhuri, S.; Lakshmi, S. A machine learning-based normalized fuzzy subset linked model in networks for intrusion detection. *Soft Computing* **2023**. https://doi.org/10.1007/s00500-023-08160-6.
15. Dhankani, M.; Rakesh, K.; Patadia, A., Intrusion Detection System Using Machine Learning. In *Advances in Data-Driven Computing and Intelligent Systems*; Springer, 2024; pp. 387–400. https://doi.org/10.1007/978-981-99-9518-9_28.
16. Amaouche, S.; Guezaz, A.; Benkirane, S.; Azrour, M.; Hazman, C., Performance Evaluation of Intrusion Detection System Using Gradient Boost. In *Artificial Intelligence, Data Science and Applications*; Springer, 2024; pp. 318–323. https://doi.org/10.1007/978-3-031-48573-2_46.
17. Saranya, R.; Priscila, S., An Optimized Hybrid Deep Learning Framework for Intrusion Detection System Integration. In *Artificial Intelligence Based Smart and Secured Applications*; Springer, 2025; pp. 42–54. https://doi.org/10.1007/978-3-031-86293-9_4.
18. Zhang, Z.; Das, A.; Huang, G.; Baskiyar, S. CAT: A simple heterogeneous ensemble learning framework for network intrusion detection. *Peer-to-Peer Networking and Applications* **2025**, *18*. https://doi.org/10.1007/s12083-025-02000-0.

 doi:10.20944/preprints202605.1231.v1

19. Chandu, S.; Anumula, R.; Chandu, P.; Varri, U. Evaluating the Effectiveness of Machine Learning Algorithms for Network Intrusion Detection. In Proceedings of the Advanced Network Technologies and Intelligent Computing. Springer, 2025, pp. 325–344. https://doi.org/10.1007/978-3-031-83783-8_19.
20. Prabhakaran, V.; Kulandasamy, A. mLBOA-DML: modified butterfly optimized deep metric learning for enhancing accuracy in intrusion detection system. *Journal of Reliable Intelligent Environments* **2023**, *9*, 333–347. https://doi.org/10.1007/s40860-022-00197-y.
21. Soltani, M.; Khajavi, K.; Jafari, M.; Jahangir, A. A multi-agent adaptive deep learning framework for online intrusion detection. *Cybersecurity* **2024**, *7*. https://doi.org/10.1186/s42400-023-00199-0.
22. Sharma, V.; Shah, D., Synergizing Machine Learning: A Comparative Exploration of Hybrid Models for Intrusion Detection. In *Artificial Intelligence and Sustainable Computing*; Springer, 2025; pp. 145–162. https://doi.org/10.1007/978-981-96-3337-1_12.
23. Yang, W.; Shan, Y.; Wang, J.; Yao, Y. An industrial network intrusion detection algorithm based on IGWO-GRU. *Cluster Computing* **2024**, *27*, 7199–7217. https://doi.org/10.1007/s10586-024-04338-1.
24. Behrens, R.; Ahmed, A. Internet of Things: An end-to-end security layer. In Proceedings of the 2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN). IEEE, 2017, pp. 146–149.
25. Abhale, A.; Avulapalli, J. Enhancing intrusion detection recursive feature elimination with resampling in WSN. *International Journal of System Assurance Engineering and Management* **2023**, *14*, 2642–2660. https://doi.org/10.1007/s13198-023-02128-3.
26. Shebl, A.; Elsedimy, E.; Ismail, A.; Salama, A.; Herajy, M. DCNN: a novel binary and multi-class network intrusion detection model via deep convolutional neural network. *EURASIP Journal on Information Security* **2024**, *2024*. https://doi.org/10.1186/s13635-024-00184-1.
27. Bowen, B.; Chennamaneni, A.; Goulart, A.; Lin, D. BLoCNet: a hybrid, dataset-independent intrusion detection system using deep learning. *International Journal of Information Security* **2023**, *22*, 893–917. https://doi.org/10.1007/s10207-023-00663-5.
28. Chaudhary, D.; Shekhawat, D.; Gupta, S.; Kalwar, A.; Mishra, N.; Nawal, M. Enhancing cybersecurity using optimized anti-interference dynamic integral neural network-based intrusion detection system. *Knowledge and Information Systems* **2025**, *67*, 5413–5435. https://doi.org/10.1007/s10115-025-02343-3.
29. Boi, B.; Cirillo, F.; De Santis, M.; Esposito, C., Anomaly-Based Intrusion Detection System Using ESP32-WROOM-DA. In *Advanced Information Networking and Applications*; Springer, 2025; pp. 417–429. https://doi.org/10.1007/978-3-031-87766-7_36.
30. Bhale, P.; Biswas, S.; Nandi, S. A hybrid IDS for detection and mitigation of sinkhole attack in 6LoWPAN networks. *International Journal of Information Security* **2023**, *23*, 915–934. https://doi.org/10.1007/s10207-023-00763-2.
31. Tuan, K.; Thai, N., Deep Packet: Deep Learning Model for Intrusion Detection. In *Intelligence of Things: Technologies and Applications*; Springer, 2024; pp. 339–348. https://doi.org/10.1007/978-3-031-75596-5_31.
32. Qutqut, M.H.; Ahmed, A.; Taqi, M.K.; Abimanyu, J.; Ajes, E.T.; Alhaj, F. A Comparative Evaluation of Snort and Suricata for Detecting Data Exfiltration Tunnels in Cloud Environments. *Journal of Cybersecurity and Privacy* **2026**, *6*, 17.
33. Yzzogh, H.; Benaboud, H. A comprehensive overview of machine learning for intrusion detection in software-defined networking. *Innovations in Systems and Software Engineering* **2025**, *21*, 397–419. https://doi.org/10.1007/s11334-025-00604-6.
34. Shafieian, S.; Zulkernine, M. Multi-layer stacking ensemble learners for low footprint network intrusion detection. *Complex & Intelligent Systems* **2022**, *9*, 3787–3799. https://doi.org/10.1007/s40747-022-00809-3.
35. Verma, N.; Kumar, N.; Kumar, G.; Singh, K. A hybrid ensemble framework with particle swarm optimization for network anomaly detection. *Discover Applied Sciences* **2025**, *7*. https://doi.org/10.1007/s42452-025-07419-x.
36. El-Dalahmeh, A.; Li, J.; El-Dalahmeh, G.; Razzaque, M.; Tan, Y.; Chang, V., An Intrusion Detection System Using the XGBoost Algorithm for SDVN. In *Advances in Computational Intelligence Systems*; Springer, 2024; pp. 390–402. https://doi.org/10.1007/978-3-031-47508-5_31.
37. Maheswaran, N.; Bose, S.; Prabhu, D.; Logeswari, G.; Anitha, T.; Vijayalakshmi, S., Next-Generation Hybrid IDS in SDN: Leveraging Deep Learning for Superior Threat Detection. In *Evolutionary Artificial Intelligence*; Springer, 2025; pp. 99–113. https://doi.org/10.1007/978-981-96-5210-5_8.

 doi:10.20944/preprints202605.1231.v1

38. Mahesh, D.; Tallapally, S. Advanced SDN-based network security: an ensemble optimized deep learning-based framework for mitigating DDoS attacks with intrusion detection. *Cluster Computing* **2025**, *28*. https://doi.org/10.1007/s10586-024-04989-0.
39. Sasode, S.; Upadhyay, L.; Tiwari, B.; Sharma, A., Resource-Optimised Solutions for Effective Network Intrusion Detection Systems in Cloud Environments. In *Information Systems for Intelligent Systems*; Springer, 2025; pp. 599–610. https://doi.org/10.1007/978-981-96-1747-0_49.
40. Salvakkam, D.; Saravanan, V.; Jain, P.K.; Pamula, R. Enhanced Quantum-Secure Ensemble Intrusion Detection Techniques for Cloud Based on Deep Learning. *Cognitive Computation* **2023**, *15*, 1593–1612. https://doi.org/10.1007/s12559-023-10139-2.
41. Saikam, J.; Ch, K. An ensemble approach-based intrusion detection system utilizing ISHO-HBA and SE-ResNet152. *International Journal of Information Security* **2023**, *23*, 1037–1054. https://doi.org/10.1007/s10207-023-00777-w.
42. Salim, Z.; Hasoon, S., Improving Machine Learning-Based Intrusion Detection Systems: A Comparative Study on NSL-KDD Dataset. In *Innovations of Intelligent Informatics, Networking, and Cybersecurity*; Springer, 2025; pp. 213–229. https://doi.org/10.1007/978-3-031-81065-7_14.
43. Srivastav, N.; Singh, R. An Optimized Machine Learning Based Network Intrusion Detection Systems for Identification of Low-Occurrence Attacks. *SN Computer Science* **2025**, *6*. https://doi.org/10.1007/s42979-025-04336-z.
44. Liu, Y.; Lin, Q., Deep Learning Instrusion Detection Research Based on SVMSMOTE. In *LISS 2024*; Springer, 2025; pp. 485–496. https://doi.org/10.1007/978-981-96-9697-0_38.
45. Tamilkodi, R.; Sri, P.; Balasankar, V.; Suseela, D., A Unique Imbalanced Network Traffic-Based Algorithm Related to Deep Learning and Machine Learning Techniques. In *Information System Design: AI and ML Applications*; Springer, 2024; pp. 473–484. https://doi.org/10.1007/978-981-97-6581-2_39.
46. Chen, X.; Zhang, Y.; Gong, Z.; Shi, Q.; Gong, S.; Li, Z.; Huang, D.; Jiang, N. Agm-c3banet: a network intrusion detection model for imbalanced data. *Cluster Computing* **2025**, *28*. https://doi.org/10.1007/s10586-025-05194-3.
47. Chakravarty, S.; Satpati, S.; Das, S.; Mallick, C.; Basak, K.; Majumdar, A. DLC-IDS: a novel democratic leadership classification model for intrusion detection systems. *The Journal of Supercomputing* **2025**, *81*. https://doi.org/10.1007/s11227-025-07336-1.
48. Abu-Shareha, A.A.; Abualhaj, M.M., Improving Intrusion Detection System Using Feature Weighting. In *Soft Computing and Its Engineering Applications*; Springer, 2025; pp. 147–160. https://doi.org/10.1007/978-3-031-88042-1_12.
49. Li, J.; Zhang, H.; Liu, Y.; Liu, Z. Semi-supervised machine learning framework for network intrusion detection. *The Journal of Supercomputing* **2022**, *78*, 13122–13144. https://doi.org/10.1007/s11227-022-04390-x.
50. Thaljaoui, A. Intelligent network intrusion detection system using optimized deep CNN-LSTM with UNSW-NB15. *International Journal of Information Technology* **2025**. https://doi.org/10.1007/s41870-025-02416-0.
51. Chowdhury, R.; Sen, S.; Roy, A.; Saha, B. An optimal feature based network intrusion detection system using bagging ensemble method for real-time traffic analysis. *Multimedia Tools and Applications* **2022**, *81*, 41225–41247. https://doi.org/10.1007/s11042-022-12330-3.
52. Mandela, N.; Etyang, F. Comparative analysis of deep learning models for effective denial of service (DoS) attack detection in network security. *Journal of Electrical Systems and Information Technology* **2025**, *12*. https://doi.org/10.1186/s43067-025-00267-0.
53. Sharma, H.; Singh, K. Intrusion detection system: a deep neural network-based concatenated approach. *The Journal of Supercomputing* **2024**, *80*, 13918–13948. https://doi.org/10.1007/s11227-024-05994-1.
54. Kurra, S.; Rayana, L.; Yoosuf, M., Analyzing Artificial Intelligence Based Intrusion Detection System in Detecting DDoS Attack. In *Intelligent System and Data Analysis*; Springer, 2025; pp. 237–251. https://doi.org/10.1007/978-981-97-5200-3_17.
55. Gajjar, H.; Malek, Z., Working of Convolutional Neural Network (CNN) in Network Intrusion Detection System. In *ICT Analysis and Applications*; Springer, 2025; pp. 35–41. https://doi.org/10.1007/978-981-97-9526-0_4.
56. Farhan, S.; Mubashir, J.; Haq, Y.; Mahmood, T.; Rehman, A. Enhancing network security: an intrusion detection system using residual network-based convolutional neural network. *Cluster Computing* **2025**, *28*. https://doi.org/10.1007/s10586-025-05156-9.
57. Rana, A.; Rawat, P.; Vats, S.; Sharma, V. Heatmap-Based Deep Learning Model for Network Attacks Classification. *SN Computer Science* **2024**, *5*. https://doi.org/10.1007/s42979-024-03447-3.

 doi:10.20944/preprints202605.1231.v1

58. Kushal, S.; Shanmugam, B.; Sundaram, J.; Thennadil, S. Self-healing hybrid intrusion detection system: an ensemble machine learning approach. *Discover Artificial Intelligence* **2024**, *4*. https://doi.org/10.1007/s44163-024-00120-9.
59. Liu, W.; Chen, J.; Qiu, X., CRNN-SA: A Network Intrusion Detection Method Based on Deep Learning. In *Advanced Data Mining and Applications*; Springer, 2023; pp. 471–485. https://doi.org/10.1007/978-3-031-46664-9_32.
60. Yu, J.; Hu, J.; Zeng, Y., Deep Learning Based Network Intrusion Detection. In *Computer Science and Education. Computer Science and Technology*; Springer, 2024; pp. 125–136. https://doi.org/10.1007/978-981-97-0730-0_12.
61. Naz, A.; Ullah, I.; Jonath, K.; Uzair, M.; Nizamani, A.H.; Mushtaq, H. Innovative cybersecurity solutions: a deep learning-driven model for accurate intrusion detection in network traffic. *Cluster Computing* **2025**, *28*. https://doi.org/10.1007/s10586-025-05351-8.
62. Meddeb, R.; Jemili, F.; Triki, B.; Korbaa, O. A deep learning-based intrusion detection approach for mobile Ad-hoc network. *Soft Computing* **2023**, *27*, 9425–9439. https://doi.org/10.1007/s00500-023-08324-4.
63. Tamirat, M.; Girma, A., Improving Cybersecurity Posture with Machine Learning-Based IDS Solutions. In *Intelligent Systems and Applications*; Springer, 2025; pp. 684–694. https://doi.org/10.1007/978-3-031-99965-9_42.
64. Chen, H.; Wang, Y.; Zhai, S.; Bai, W.; Diao, Z.; An, D., Artificial Intelligence-Driven Network Intrusion Detection and Response System. In *Cyber Security Intelligence and Analytics*; Springer, 2025; pp. 508–518. https://doi.org/10.1007/978-3-031-88287-6_48.
65. Barik, K.; Misra, S. A comprehensive defense approach of deep learning-based NIDS against adversarial attacks. *Multimedia Tools and Applications* **2025**, *84*, 37745–37791. https://doi.org/10.1007/s11042-025-21008-5.
66. Awad, O.; Çevik, M.; Farhan, H. An enhanced attention and dilated convolution-based ensemble model for network intrusion detection system against adversarial evasion attacks. *Peer-to-Peer Networking and Applications* **2025**, *18*. https://doi.org/10.1007/s12083-024-01859-9.
67. Kumar, S.; Bharti, S.; Singh, R.; Kumar, K.; Khari, M., Adversarial Attack Detection in Intrusion Detection System Using Machine Learning. In *Intelligent Human Computer Interaction*; Springer, 2025; pp. 426–434. https://doi.org/10.1007/978-3-031-88705-5_35.
68. Chalé, M.; Cox, B.; Weir, J.; Bastian, N. Constrained optimization based adversarial example generation for transfer attacks in network intrusion detection systems. *Optimization Letters* **2023**, *18*, 2169–2188. https://doi.org/10.1007/s11590-023-02007-7.
69. Samha, A.; Malik, N.; Sharma, D.; S, K.; Dutta, P. Intrusion Detection System Using Hybrid Convolutional Neural Network. *Mobile Networks and Applications* **2023**, *29*, 1719–1731. https://doi.org/10.1007/s11036-023-02223-6.
70. Chatterjee, S.; Shaw, V.; Das, R. Multi-stage intrusion detection system aided by grey wolf optimization algorithm. *Cluster Computing* **2023**, *27*, 3819–3836. https://doi.org/10.1007/s10586-023-04179-4.
71. Sahib, W.M.; Alhuseen, Z.A.A.; Saeedi, I.D.I.; Abdulkadhem, A.A.; Ahmed, A. Leveraging machine learning for enhanced cybersecurity: an intrusion detection system. *Service Oriented Computing and Applications* **2024**, *19*, 107–124. https://doi.org/10.1007/s11761-024-00435-6.
72. Mamatha, P.; Balaji, S.; Anuraghav, S. Development of Hybrid Intrusion Detection System Leveraging Ensemble Stacked Feature Selectors and Learning Classifiers to Mitigate the DoS Attacks. *International Journal of Computational Intelligence Systems* **2025**, *18*. https://doi.org/10.1007/s44196-025-00750-6.
73. Yu, W.; Chen, Z.; Wang, H.; Miao, Z.; Zhong, D. Industrial network intrusion detection in open-set scenarios. *International Journal of Information Security* **2024**, *24*. https://doi.org/10.1007/s10207-024-00949-2.
74. Tüzün, M.N.B.; Angin, P., Network Intrusion Detection with Incremental Active Learning. In *Advanced Information Networking and Applications*; Springer, 2024; pp. 344–353. https://doi.org/10.1007/978-3-031-57942-4_33.
75. Hariharan, S.; Rejimol Robinson, R.; Prasad, R.; Thomas, C.; Balakrishnan, N. XAI for intrusion detection system: comparing explanations based on global and local scope. *Journal of Computer Virology and Hacking Techniques* **2022**, *19*, 217–239. https://doi.org/10.1007/s11416-022-00441-2.
76. Sivamohan, S.; Sridhar, S.S. An optimized model for network intrusion detection systems in industry 4.0 using XAI based Bi-LSTM framework. *Neural Computing and Applications* **2023**, *35*, 11459–11475. https://doi.org/10.1007/s00521-023-08319-0.

 doi:10.20944/preprints202605.1231.v1

77. Reddy, P.; Upadhyay, L.; Rakesh, L., Performance Analysis of Machine Learning Classifiers on CICIDS2017 Dataset. In *Intelligent Solutions for Smart Adaptation in Digital Era*; Springer, 2025; pp. 365–382. https://doi.org/10.1007/978-981-97-8193-5_30.
78. Zabawa, P.; Kedziora, M., Analysis of Network Intrusion Detection and Potential Botnets Identification Using Selected Machine Learning Techniques. In *Advances in Computational Collective Intelligence*; Springer, 2024; pp. 43–53. https://doi.org/10.1007/978-3-031-70259-4_4.
79. Pingili, M.; Sravanthi, G.; Srujan Raju, K.; Rajesh, V.; Deepika, A.; Patel, P., A Novel Approach of Enhancing and Developing IDS to Use Ml for Analyzing Malicious Attacks. In *Innovations in Information and Decision Sciences*; Springer, 2025; pp. 377–385. https://doi.org/10.1007/978-981-96-0147-9_31.
80. Khalid, M.; Mohsin, A.; Ali, J.; Roh, B.h. Optimization of recurrent neural networks for high-performance intrusion detection in network traffic. *Cluster Computing* **2025**, *28*. https://doi.org/10.1007/s10586-025-05240-0.
81. Harish, R.; Suresh, S.; Sai, S.; Deepa, R., Network Anomaly Detection Mitigation of DDoS Attack Using Machine Learning. In *Computing Technologies for Sustainable Development*; Springer, 2025; pp. 80–92. https://doi.org/10.1007/978-3-031-82383-1_7.
82. Gupta, H.; Arora, D.; Tiwari, S., Leveraging Machine Learning Algorithms for Enhanced Network Intrusion Detection and Categorization (NIDC). In *Cyber Security and Digital Forensics*; Springer, 2025; pp. 79–89. https://doi.org/10.1007/978-981-96-3284-8_6.
83. Nguyen, X.H.; Nguyen, X.D.; Le, K.H., Preventing Adversarial Attacks Against Deep Learning-Based Intrusion Detection System. In *Information Security Practice and Experience*; Springer International Publishing, 2022; pp. 382–396. https://doi.org/10.1007/978-3-031-21280-2_21.
84. Johnson Singh, K.; Maisnam, D.; Chanu, U.S. Intrusion Detection System with SVM and Ensemble Learning Algorithms. *SN Computer Science* **2023**, *4*. https://doi.org/10.1007/s42979-023-01954-3.
85. Jain, J.; Chauhan, D., Decision Tree Based Network Intrusion Detection for Cyber Security Application. In *Innovations in Data Analytics*; Springer, 2024; pp. 417–426. https://doi.org/10.1007/978-981-97-3466-5_31.
86. Jahan, T.; Reddy, A.; Sinjini, J.; Priyadharshini, M.; Indumathi, V.; Bhavani, V., Methods and Techniques of Cybersecurity Intrusion Detection: Supervised Machine Learning. In *Proceedings of the Third International Conference on Cognitive and Intelligent Computing, Volume 1*; Springer, 2025; pp. 691–709. https://doi.org/10.1007/978-981-97-9262-7_60.
87. Hossen, M.; Rumpa, U.; Huque, M.; Fokir, M.; Uddin, F.; Salsabin, N.; Hossain, M.; Reza, A., Analyzing the Effectiveness of Machine Learning Algorithms in Intrusion Detection. In *Data Mining and Information Security*; Springer, 2025; pp. 59–70. https://doi.org/10.1007/978-981-96-6063-6_5.
88. Hong, L.; Aslam, S.; Majeed, A.; Teh, S.H., Machine Learning Approaches for Effective Intrusion Detection Systems. In *Selected Proceedings from the 2nd International Conference on Intelligent Manufacturing and Robotics, ICIMR 2024, 22-23 August, Suzhou, China*; Springer, 2025; pp. 410–419. https://doi.org/10.1007/978-981-96-3949-6_33.
89. Rajwar, S.; Manjhi, P.; Mukherjee, I., Comparative Evaluation of Machine Learning Methods for Network Intrusion Detection System. In *Intelligent Systems and Sustainable Computing*; Springer, 2022; pp. 531–541. https://doi.org/10.1007/978-981-19-0011-2_47.
90. Peter, S.; Aravind, J.; Jacob, F.; George, J.V.; Mathew, T., Real-Time Network Intrusion Detection System Using Machine Learning. In *Demystifying AI and ML for Cyber–Threat Intelligence*; Springer, 2025; pp. 67–87. https://doi.org/10.1007/978-3-031-90723-4_6.
91. Phulre, A.; Verma, M.; Mathur, J.; Jain, S., Approach on Machine Learning Techniques for Anomaly-Based Web Intrusion Detection Systems: Using CICIDS2017 Dataset. In *Machine Intelligence for Research and Innovations*; Springer, 2024; pp. 59–72. https://doi.org/10.1007/978-981-99-8135-9_6.
92. Pameela Rani, P.; Vidhya, S., An Efficient Intrusion Detection System Using Deep Learning Techniques. In *Artificial Intelligence Based Smart and Secured Applications*; Springer, 2025; pp. 335–347. https://doi.org/10.1007/978-3-031-86299-1_24.
93. Möller, D., Machine Learning and Deep Learning. In *Guide to Cybersecurity in Digital Transformation*; Springer, 2023; pp. 347–384. https://doi.org/10.1007/978-3-031-26845-8_8.
94. Menon, V.; Palivela, L., A Stacked Ensemble Learning Model for Enhanced Network Intrusion Detection. In *Soft Computing and Signal Processing*; Springer, 2025; pp. 309–324. https://doi.org/10.1007/978-981-96-0924-6_25.
95. Manzoor, S.; Ahmad, M.; Alhadawi, H.S., Intrusion Detection System Using Ensemble Machine Learning in Cloud Environment. In *Proceedings of the 2nd International Conference on Emerging Technologies and Intelligent*

 doi:10.20944/preprints202605.1231.v1

Systems; Springer International Publishing, 2023; pp. 513–522. https://doi.org/10.1007/978-3-031-25274-7_43.

96. Ahmad, T.; Truscan, D.; Vain, J., EARLY: A Tool for Real-Time Security Attack Detection. In *CyberSecurity in a DevOps Environment*; Springer, 2023; pp. 225–251. https://doi.org/10.1007/978-3-031-42212-6_8.
97. Rizvi, S.; Scanlon, M.; McGibney, J.; Sheppard, J., Deep Learning Based Network Intrusion Detection System for Resource-Constrained Environments. In *Digital Forensics and Cyber Crime*; Springer, 2023; pp. 355–367. https://doi.org/10.1007/978-3-031-36574-4_21.
98. Talukder, M.; Sharmin, S.; Uddin, M.; Islam, M.; Aryal, S. MLSTL-WSN: machine learning-based intrusion detection using SMOTETomek in WSNs. *International Journal of Information Security* **2024**, *23*, 2139–2158. https://doi.org/10.1007/s10207-024-00833-z.
99. T., G.; A., D.; M, M. Deep learning method for efficient cloud IDS utilizing combined behavior and flow-based features. *Applied Intelligence* **2024**, *54*, 6738–6759. https://doi.org/10.1007/s10489-024-05505-y.
100. Alshaya, R.; AL Khediri, S. Optimizing cybercrime detection: A hybrid deep learning approach for enhanced intrusion detection systems. *Peer-to-Peer Networking and Applications* **2025**, *18*. https://doi.org/10.1007/s12083-025-01933-w.
101. Al-Absi, M.; R'bigui, S.; Sain, M.; Al-Absi, A.; Lee, H., A Comparative Evaluation of Deep Learning Algorithms: Assessing Effectiveness and Performance. In *Proceedings of 3rd International Conference on Smart Computing and Cyber Security*; Springer, 2024; pp. 157–168. https://doi.org/10.1007/978-981-97-0573-3_13.
102. Akanksha, P.; Manohar Naik, S., Network Intrusion Detection with SMOTE-ENN and Deep Learning Techniques. In *Smart Computing Paradigms: Artificial Intelligence and Network Applications*; Springer, 2024; pp. 57–67. https://doi.org/10.1007/978-981-97-7880-5_6.
103. Lavaniya, S.; Jain, S. Deep Neural Network Based Cyber Intrusion Detection System. In Proceedings of the 3rd International Conference on Disruptive Technologies (ICDT), March 2025, pp. 212–217. https://doi.org/10.1109/ICDT63985.2025.10986305.
104. El Asry, C.; Douzi, S.; El Ouahidi, B., A Deep Learning Model for Intrusion Detection with Imbalanced Dataset. In *Advances in Intelligent System and Smart Technologies*; Springer International Publishing, 2024; pp. 261–271. https://doi.org/10.1007/978-3-031-47672-3_26.
105. Deore, B.; Bhosale, S. Adaptive Dolphin Atom Search Optimization-Based DRNN for Network Intrusion Detection System. *SN Computer Science* **2023**, *4*. https://doi.org/10.1007/s42979-023-02006-6.
106. Deng, L.; Zhao, Y.; Bao, H., A Self-supervised Adversarial Learning Approach for Network Intrusion Detection System. In *Cyber Security*; Springer, 2022; pp. 73–85. https://doi.org/10.1007/978-981-19-8285-9_5.
107. Kashyap, A.; Singh, V.; Garg, M., Multi-Layered Intrusion Detection System Using Ensemble Learning. In *Intelligent Strategies for ICT*; Springer, 2025; pp. 425–435. https://doi.org/10.1007/978-981-96-5607-3_37.
108. Muhammad, A.; Murtza, I.; Saadia, A.; Kifayat, K. Cortex-inspired ensemble based network intrusion detection system. *Neural Computing and Applications* **2023**, *35*, 15415–15428. https://doi.org/10.1007/s00521-023-08561-6.
109. Maske, S.; Rane, S.; Bhalkare, P.; Aylani, A.; Shrivastava, S.; Dutta, P., Intelligent Machine Learning for Cybersecurity: Anomaly Detection in Network Intrusion Systems and Beyond. In *Electronic Governance with Emerging Technologies*; Springer, 2024; pp. 137–146. https://doi.org/10.1007/978-3-031-77029-6_11.
110. Mo, J.; Ke, J.; Zhou, H.; Li, X. Hybrid network intrusion detection system based on sliding window and information entropy in imbalanced dataset. *Applied Intelligence* **2025**, *55*. https://doi.org/10.1007/s10489-025-06307-6.
111. Mondragon, J.; Branco, P.; Jourdan, G.V.; Gutierrez-Rodriguez, A.E.; Biswal, R. Advanced IDS: a comparative study of datasets and machine learning algorithms for network flow-based intrusion detection systems. *Applied Intelligence* **2025**, *55*. https://doi.org/10.1007/s10489-025-06422-4.
112. Li, X.; Li, L., Research on Multi-level Classification Models for Imbalanced Network Intrusion Dataset. In *Proceedings of the 6th International Conference on Electronic Information Technology and Computer Engineering*; Association for Computing Machinery (ACM): New York, NY, USA, 2023; pp. 967–972. https://doi.org/10.1145/3573428.3573603.
113. Gjorgjievska, M.; Dimitrova, V., Application of Machine Learning in Intrusion Detection Systems. In *Intelligent Computing*; Springer, 2023; pp. 1288–1308. https://doi.org/10.1007/978-3-031-37717-4_86.
114. Getman, A.; Rybolovlev, D.; Nikolskaya, A. Deep Learning Applications for Intrusion Detection in Network Traffic. *Programming and Computer Software* **2024**, *50*, 493–510. https://doi.org/10.1134/s0361768824700221.

 doi:10.20944/preprints202605.1231.v1

115. Giagkos, D.; Kompougias, O.; Litke, A.; Papadakis, N., ZeekFlow: Deep Learning-Based Network Intrusion Detection a Multimodal Approach. In *Computer Security. ESORICS 2023 International Workshops*; Springer, 2024; pp. 409–425. https://doi.org/10.1007/978-3-031-54129-2_24.
116. Saila, B.; Emmanuel, A.; Teja, E.; Kokatnoor, S.A.; Mandala, J.; Kumar, S., Machine Learning in Intrusion Detection: A Comprehensive Analysis. In *Data Science and Applications*; Springer, 2025; pp. 591–603. https://doi.org/10.1007/978-981-96-2299-3_40.
117. Singh, B.; Indu, S.; Majumdar, S. Comparative Analysis of Intrusion Detection Models Using Quantum Machine Learning Techniques. *Circuits, Systems, and Signal Processing* **2025**. https://doi.org/10.1007/s00034-025-03256-w.
118. Sood, I.; Sharma, V., Computational Intelligence Approach for an Intrusion Detection System. In *Advanced Network Technologies and Computational Intelligence*; Springer, 2025; pp. 239–253. https://doi.org/10.1007/978-3-031-86069-0_19.
119. Tharun, J.; Arumugam, S., Performance Analysis of Network Intrusion Detection System Using Naïve Bayes Algorithm in Comparison with One-Class Learning. In *Innovations in Knowledge Mining: Sustainability for Societal and Industrial Impact*; Springer, 2025; pp. 557–563. https://doi.org/10.1007/978-981-96-5217-4_46.
120. Tayal, P.; Kumar, R.; Hemlata., A Comparative Evaluation of Machine Learning Techniques for Detecting Malicious Network Traffic. In *Computation of Artificial Intelligence and Machine Learning*; Springer, 2024; pp. 184–204. https://doi.org/10.1007/978-3-031-71481-8_15.
121. Wang, J.; Yang, K.; Cong, W.; Li, M.; Bai, L.; Wang, X., High-Precision Network Intrusion Detection Method Based on NIDS-CNNRF. In *Advanced Information Networking and Applications*; Springer, 2025; pp. 234–243. https://doi.org/10.1007/978-3-031-87772-8_20.
122. Wang, J.; Yang, K.; Cong, W.; Li, M.; Bai, L.; Wang, X., Network Intrusion Detection Based on CNN-BiGRU. In *Advanced Information Networking and Applications*; Springer, 2025; pp. 62–71. https://doi.org/10.1007/978-3-031-87781-0_7.
123. Wang, Y.; Zhang, Z.; Zhao, K.; Wang, P.; Wu, R. A few-shot learning based method for industrial internet intrusion detection. *International Journal of Information Security* **2024**, *23*, 3241–3252. https://doi.org/10.1007/s10207-024-00889-x.
124. Wang, H.; Zhou, S.; Li, H.; Hu, J.; Du, X.; Zhou, J.; He, Y.; Fu, F.; Yang, H., Deep Learning Network Intrusion Detection Based on Network Traffic. In *Artificial Intelligence and Security*; Springer International Publishing, 2022; pp. 194–207. https://doi.org/10.1007/978-3-031-06791-4_16.
125. Xie, L.; Ye, M.; Chen, B., A Network Intrusion Detection System Based on Self-supervised Co-contrastive Learning. In *Network Simulation and Evaluation*; Springer, 2024; pp. 387–399. https://doi.org/10.1007/978-981-97-4522-7_27.
126. Winiecki, E.; Pawlicki, M.; Pawlicka, A.; Kozik, R.; Choraś, M., Evaluation of Selected Few-Shot Learning Methods in Network Intrusion Detection. In *Advanced Information Networking and Applications*; Springer, 2025; pp. 10–20. https://doi.org/10.1007/978-3-031-87778-0_2.
127. Vadhil, F.; Nanne, M.; Salihi, M., A Novel Artificial Intelligence-Based Intrusion Detection System—NAI2DS. In *Artificial Intelligence and Its Practical Applications in the Digital Economy*; Springer, 2024; pp. 168–181. https://doi.org/10.1007/978-3-031-71426-9_14.
128. Tumkur, S.; Eswarakrishnan, V.; Wairagade, A.; Aslam, M.; Bilal, M.; Cheema, A. Optimizing Malware Detection in Virtual Cloud Environments Using Hybrid Machine Learning Approach. *Arabian Journal for Science and Engineering* **2025**. https://doi.org/10.1007/s13369-025-10205-x.
129. Kulkarni, G.; Rathore, M., Deep Learning Methods for Network Intrusion Detection Systems. In *Business Intelligence, Computational Mathematics, and Data Analytics*; Springer, 2025; pp. 95–106. https://doi.org/10.1007/978-3-031-87511-3_7.
130. Bushra, S.; Subramanian, N.; Chandrasekar, A. An optimal and secure environment for intrusion detection using hybrid optimization based ResNet 101-C model. *Peer-to-Peer Networking and Applications* **2023**, *16*, 2307–2324. https://doi.org/10.1007/s12083-023-01500-1.