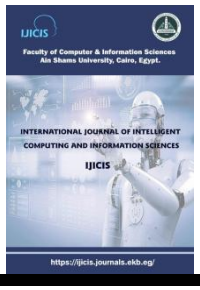
IJICIS, Vol.25, No.2, 74-87
DOI: 10.21608/ijicis.2025.395907.1404

International Journal of Intelligent Computing and Information Sciences

https://ijicis.journals.ekb.eg/



DEEP LEARNING TECHNIQUES FOR NETWORK INTRUSION DETECTION: A COMPARATIVE SURVEY

Alaa Prince AbdelHalim*
Cyber Security Department,
Faculty of Computer and Information Sciences,
Ain Shams University,
Cairo, Egypt
alaaprince@cis.asu.edu.eg

Alshaimaa Abo-Alian
Information Systems Department,
Faculty of Computer and Information Sciences,
Ain Shams University,
Cairo, Egypt
a_alian@cis.asu.edu.eg

Nagwa Badr
Information Systems Department,
Faculty of Computer and Information Sciences,
Ain Shams University,
Cairo, Egypt
nagwabadr@cis.asu.edu.eg

Received 2025-06-19; Revised 2025-06-19; Accepted 2025-07-03

Abstract: *The growing complexity and scale of cyberattacks have driven the evolution of Network Intrusion Detection Systems from traditional signature-based methods to deep learning-driven approaches capable of detecting novel and adversarial threats. This survey presents a comprehensive analysis of recent advances in flow-based and packet-based NIDS, with a focus on robustness, real-time performance, and adaptability to zero-day and adversarial attacks. State-of-the-art methods have been examined in each category, covering a diverse range of deep learning architectures including Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTMs), transformers, federated learning frameworks, and adversarial training techniques. The surveyed works are evaluated based on data modality, learning paradigm, deployment setting, detection capability, and resilience against evolving threats. Through structured taxonomy and comparative analysis, Key strengths, limitations, and performance trade-offs between flow-level and packet-level systems have been highlighted. Finally, open research challenges have been identified such as data heterogeneity, explainability, and adversarial robustness, and propose future directions for building adaptive and trustworthy intrusion detection systems suitable for real-world deployment.*

Keywords: *Network Intrusion Detection, Machine Learning, Flow-based Detection, Packet-based Detection.*

1. Introduction

The rapid evolution of cyber threats, characterized by increasing sophistication and scale, has underscored the critical need for robust Network Intrusion Detection Systems (NIDS) [1]. Traditional signature-based NIDS, while effective against known attack patterns, often fall short in detecting novel,

***Corresponding Author**: Alaa Prince AbdelHalim

Cyber Security Department, Faculty of Computer and Information Science, Ain Shams University, Cairo, Egypt

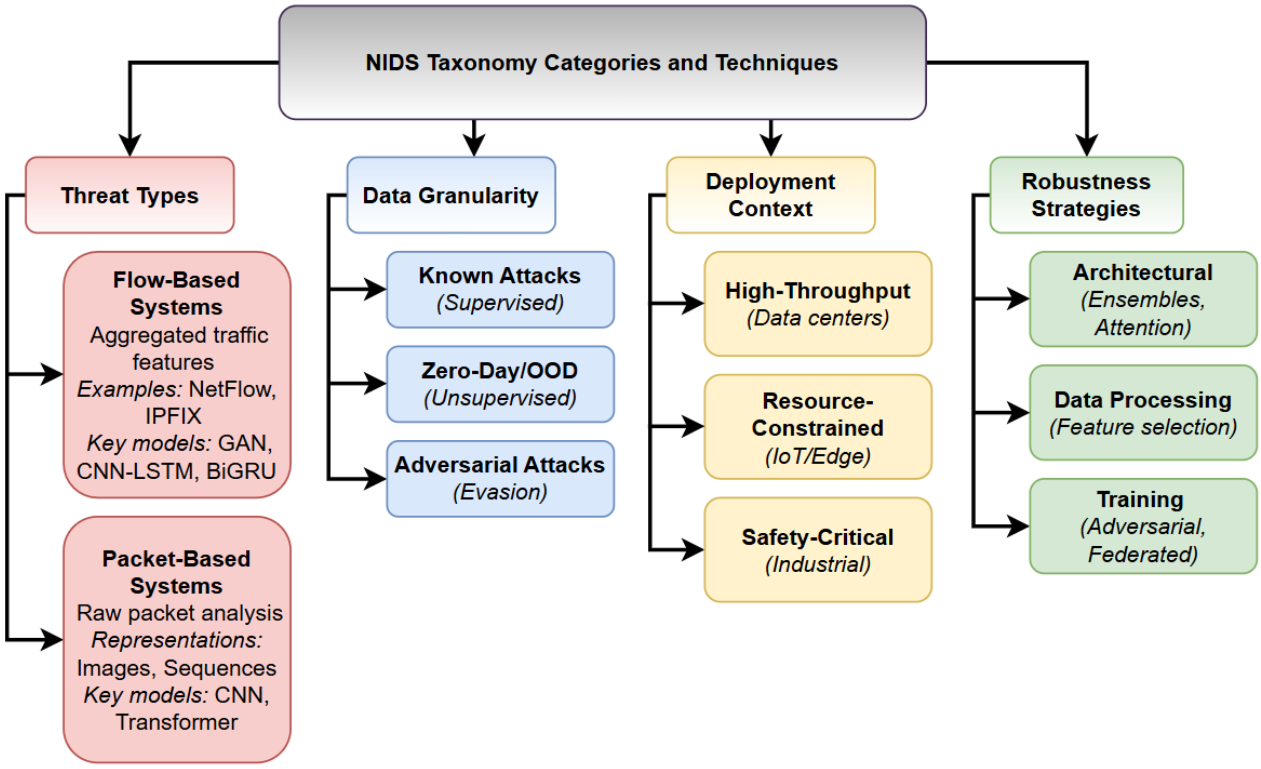
Email address: alaaprince@cis.asu.edu.eg

zero-day, and adversarial attacks due to their reliance on predefined rules and signatures [2]. This limitation has propelled the research community towards leveraging advanced machine learning (ML) and deep learning (DL) techniques to develop more intelligent, adaptive, and resilient NIDS. These modern systems typically process network traffic data in two primary forms: flow-based data, which aggregates network traffic into summarized records, and packet-based data, which involves the direct analysis of raw or minimally pre-processed individual packet information [3]. Both flow-based and packet-based approaches offer distinct advantages and present unique challenges. Flow-based systems are inherently scalable and efficient, making them suitable for high-throughput network environments like data centers and industrial networks [4]. They derive insights from aggregated statistical features over defined time intervals, allowing for broad-spectrum anomaly detection. However, their aggregated nature can limit their effectiveness in identifying subtle, low-and-slow, or stealthy attacks that may not significantly alter flow-level statistics. Conversely, packet-based systems provide a finer granularity of analysis by examining the raw contents and structures of individual packets. This allows for superior sensitivity to subtle anomalies and early-stage intrusions, including those embedded within encrypted traffic through behavioral or side-channel analysis. Nevertheless, packet-based approaches often incur substantial preprocessing costs and face scalability issues in high-velocity network settings, alongside challenges posed by the increasing prevalence of encrypted traffic [5]. Recent advancements in deep learning, including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs) such as Long Short-Term Memory (LSTMs) and Gated Recurrent Unit (GRUs), transformers, and federated learning frameworks, have significantly enhanced the capabilities of both flow-based and packet-based NIDS [6]. These techniques have improved detection accuracy, generalizability, and robustness against evolving threats. Furthermore, the integration of adversarial learning and novel training paradigms is increasingly crucial for defending against sophisticated evasion tactics. [7] Despite these advancements, the performance and practicality of these systems vary widely depending on factors such as the dataset used, system architecture, attack model, and deployment constraints.

This survey presents a comprehensive and comparative analysis of recent deep learning-based Network Intrusion Detection System approaches, categorized primarily by data granularity: flow-based and packet-based. Architectural designs, feature extraction techniques, learning paradigms, attack coverage, and adversarial resilience are examined and contrasted to reveal the respective strengths and limitations of each paradigm. Promising research directions are identified, and actionable insights are provided for practitioners aiming to develop or enhance intelligent intrusion detection systems. Figure 1 illustrates a structured taxonomy of deep learning-based Network Intrusion Detection Systems (NIDS), organizing key design and operational aspects into four main categories: Threat Types, Data Granularity, Deployment Context, and Robustness Strategies. Under Threat Types, systems are divided into Flow-

Based Systems, which rely on aggregated traffic features such as NetFlow and IPFIX and use models like CNN-LSTM, BiGRU, and GAN, and Packet-Based Systems, which analyze raw packet data using image or sequence representations and typically apply CNN or Transformer architectures. The Data Granularity category covers the nature of threats targeted, including Known Attacks (supervised learning), Zero-Day or Out-of-Distribution (OOD) attacks (unsupervised learning), and Adversarial Attacks (evasion scenarios). The Deployment Context highlights the environments where NIDS may be applied, including High-Throughput settings like data centers, Resource-Constrained environments such as IoT or edge devices, and Safety-Critical industrial systems. Lastly, Robustness Strategies address system resilience through Architectural designs like attention mechanisms and ensembles, Data Processing techniques such as feature selection, and Training approaches including adversarial or federated methods. This taxonomy provides a comprehensive framework for analyzing and developing

deep learning-based NIDS solutions across multiple dimensions. Additionally, common datasets used in the field are outlined, and their structural characteristics are discussed. Particular attention is given to the challenges and future directions related to flow-based and packet-based NIDS, especially



concerning data heterogeneity, explainability, and adversarial robustness.

This paper is structured to provide a comprehensive overview of deep learning-based Network Intrusion Detection Systems. Following the introduction, Section 2 establishes a detailed taxonomy of NIDS approaches, categorizing them by data granularity (flow-based vs. packet-based) and the types of threats they address. Section 3 then delves into recent works in the field, presenting a detailed review of both flow-based and packet-based NIDS, highlighting their architectural designs, performance metrics, and inherent strengths and limitations. The paper concludes by identifying open research challenges and proposing future directions for the development of adaptive and trustworthy intrusion detection systems.

2. Taxonomy of NIDS Approaches

To effectively understand and contextualize the rapid advancements in deep learning-based Network Intrusion Detection Systems, it is essential to establish a comprehensive taxonomy. This taxonomy categorizes surveyed approaches based on several critical dimensions that profoundly influence their performance, robustness, and applicability in real-world scenarios. These dimensions include data granularity, threat types addressed, deployment context, and robustness strategies.

2.1. Data Granularity: Flow-Based vs. Packet-Based

The fundamental distinction in NIDS models lies in their operational data granularity:

Figure 1. Taxonomy of deep learning-based NIDS approaches by data granularity and threat model.

- **Flow-Based Systems:** These systems process aggregated statistical features derived from sequences of packets over defined time windows. Examples of flow data include NetFlow [8], IPFIX [9], and sFlow [10], which summarize communication sessions by capturing metadata such as source/destination IP addresses and ports, protocol, byte counts, and packet counts. This aggregation enables highly scalable analysis, making flow-based NIDS particularly suitable for high-throughput network environments where detailed packet inspection would be computationally prohibitive. While efficient for detecting large-scale anomalies and known attack patterns, their reliance on summarized data can limit their ability to identify subtle, low-frequency, or stealthy attacks that do not significantly alter flow statistics.
- **Packet-Based Systems:** In contrast, packet-based systems operate directly on the raw content or low-level features of individual network packets. This approach offers significantly higher fidelity, allowing for the detection of fine-grained anomalies, polymorphic payloads, and even patterns within encrypted traffic through techniques like traffic analysis or side-channel information. Methods often involve converting packet data into various representations, such as grayscale images [11], multi-channel image encodings of headers and payloads [12], or token sequences for transformer models [13]. While providing superior sensitivity to subtle intrusions, packet-based NIDS typically incur substantial preprocessing costs and face scalability challenges in high-velocity networks due to the sheer volume of data they must process.

Figure 2 conceptually illustrates the architectural distinction between flow-based and packet-based NIDS, emphasizing the abstraction level of data processing and the corresponding learning pipeline in each approach.

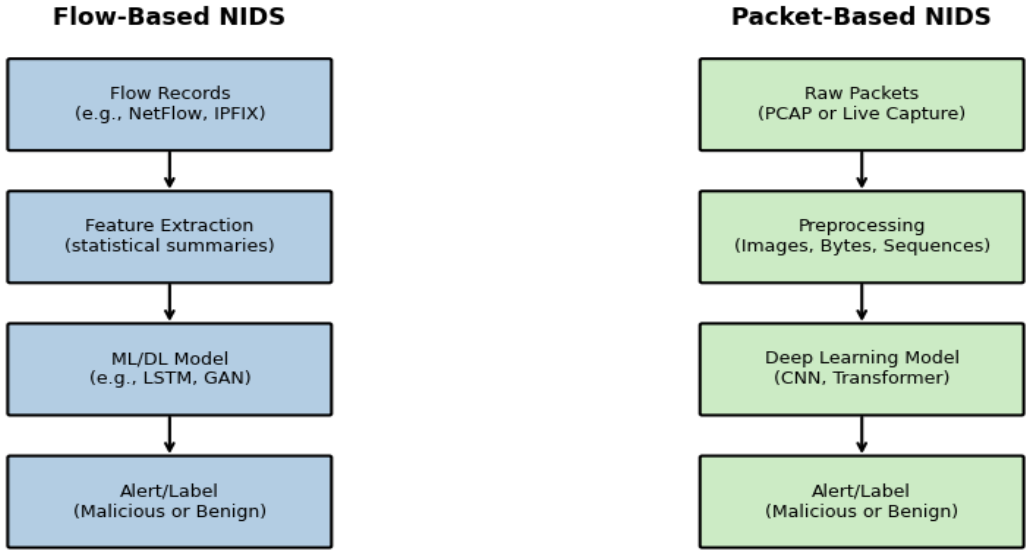


Figure 2. Flow-Based vs Packet-Based NIDS Architectural Overview

2.2. Threat Types Addressed

Modern NIDS must be capable of contending with a diverse array of cyber threats. The design of a NIDS often reflects its primary focus concerning threat types:

- **Known Attack Signatures:** Many NIDS, particularly those based on supervised learning, excel at detecting previously identified attack patterns. These systems are trained on datasets containing

labeled instances of known attacks and normal traffic. While highly accurate for recognized threats, they are inherently limited in their ability to detect novel or evolving attacks.

- **Zero-Day and Out-of-Distribution (OOD) Attacks:** A critical challenge for NIDS is the detection of zero-day exploits and attacks that deviate significantly from known patterns. Systems designed to address these threats often incorporate unsupervised learning techniques (e.g., anomaly detection, clustering), semi-supervised learning, or novelty detection mechanisms. These approaches aim to identify unusual behaviors or deviations from established baselines, thereby offering a proactive defense against unknown threats [14].
- **Adversarial Attacks:** With the increasing sophistication of attackers, NIDS are now confronted with adversarial attacks specifically designed to evade detection by manipulating input data. Robust NIDS incorporate specialized mechanisms such as adversarial training, input sanitization, feature-space regularization, and explainability-driven defenses to improve generalization and resilience against such sophisticated evasion tactics [15, 16].

3. NIDS: Recent Works

This section provides a detailed review of recent deep learning-based Network Intrusion Detection Systems, categorized by their data granularity: flow-based and packet-based. For each category, we highlight key architectural designs, datasets utilized, reported performance metrics, and inherent strengths and limitations.

3.1. Flow-Based NIDS

Flow-based NIDS leverage aggregated network traffic information to detect intrusions, offering scalability and efficiency for high-throughput environments. Recent research in this domain has explored diverse deep learning architectures to enhance detection capabilities:

- **Li et al. [17]** proposed an unsupervised Generative Adversarial Network (GAN) model for NIDS, incorporating flow encoding and adaptive thresholding. Evaluated on benchmark datasets such as NSL-KDD [18], CIC-IDS2017 [19], CIC-DDoS2019 [20], and UNSW-NB15 [21], their model demonstrated strong zero-day detection capabilities with an Area Under the Curve (AUC) approximately 0.98. However, a notable limitation of this approach is the inherent instability often associated with GAN training, which can affect its reliability and deployment in real-world scenarios.
- **Asadi et al. [22]** combined Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks for botnet recognition. Their approach utilized flow features, with dimensionality reduction achieved through Classification and Regression Trees (CART). Tested on the ISCX [23] and ISOT [24] datasets, the model achieved a precision of approximately 99.7%. Despite its high precision, the model exhibited susceptibility to advanced adversarial attacks, including Projected Gradient Descent (PGD) and Basic Iterative Method (BIM), indicating a need for enhanced adversarial robustness.
- **Awad et al. [25]** introduced an ensemble model comprising LSTM, Gated Recurrent Unit (GRU), and dilated convolutions, augmented with an attention mechanism. Feature selection was optimized using an Improved Cheetah Optimizer, leading to approximately 95% accuracy on the CIC-IDS2017 dataset. While effective, the computational demands of this ensemble approach make it challenging for real-time deployment in resource-constrained environments.
- **Emirmahmutoğlu and Atay [14]** explored the use of metaheuristic feature selection methods, specifically Particle Swarm Optimization (PSO), Flower Pollination Algorithm (FPA), and

Differential Evolution (DE), in conjunction with classical classifiers. This hybrid approach achieved near-perfect F1 scores (approximately 0.999), demonstrating high accuracy on known attack patterns. However, its adaptability to new and unseen threats remains limited, as it tends to overfit to known patterns.

- **Hu et al. [26]** developed a Bidirectional GRU (BiGRU) network integrated with a gated self-attention mechanism. To address class imbalance, they employed a hybrid resampling technique combining undersampling and K-SMOTE. This model achieved approximately 98.4% accuracy across various datasets, performing particularly well in detecting minority class intrusions. The attention mechanism enhances the model's ability to focus on relevant features, improving overall detection performance.
- **Talpini et al. [27]** applied Bayesian neural networks with Mahalanobis distance calibration to provide trustworthy uncertainty estimation for NIDS. This approach proved effective for open-set detection, allowing the system to identify novel attacks with a measure of confidence. A drawback, however, is the slower inference speed associated with Bayesian neural networks, which can impact real-time detection capabilities.
- **Khan et al. [28]** proposed an Artificial Neural Network (ANN) with genetic algorithm-based feature optimization, specifically tailored for Industrial Internet of Things (IIoT) environments. This framework achieved approximately 99.5% accuracy on IoTID20-based datasets [29]. While highly effective for IIoT, the specialized nature of this framework suggests it may not generalize well to broader network environments.

3.2. Packet-Based NIDS

Packet-based NIDS analyze raw packet content to identify intrusions, offering fine-grained detection capabilities crucial for subtle or low-volume attacks. Research in this area has focused on innovative data representations and advanced deep learning architectures:

- **Hore et al. [11]** converted network packets into grayscale images, which were then analyzed using CNNs over five-packet windows. This method achieved 99.7% accuracy on CIC-IDS2017, enhancing spatial learning for intrusion detection. A practical consideration for this approach is the need for efficient PCAP (Packet Capture) handling to manage the large volume of raw packet data.
- **Doriguzzi Corin et al. [12]** applied multi-channel image encodings of packet headers and payloads, combined with hybrid CNN-BiLSTM models. This approach yielded approximately 98% F1 score on several datasets, demonstrating its effectiveness in capturing both spatial and sequential patterns within packet data. However, the encoding process itself incurs significant computational costs, which can impact real-time performance.
- **Nguyen et al. [13]** modeled network packets as token sequences, processing them with transformer encoders. This method achieved approximately 99% accuracy on multiple datasets, showcasing the power of transformer architectures in capturing long-range dependencies within packet flows. A major challenge with this approach is the high memory usage associated with transformer models, which can be a limiting factor for deployment in environments with constrained resources.
- **Hore et al. [15]** augmented packet images using various techniques such as noise, flips, and rotation, and paired them with ResNet-based CNNs. This augmentation strategy aimed to improve robustness against minor obfuscations in network traffic. While effective in enhancing resilience, the introduction of augmentation artifacts can sometimes negatively affect the model's overall performance.

- **Verma et al. [30]** demonstrated few-shot classification using prototypical networks on byte sequences extracted from PCAPs. This approach performed well with minimal training data, making it suitable for scenarios where labeled data is scarce. However, it struggled with detecting subtle variations in attack patterns, indicating a potential limitation in its ability to generalize to highly nuanced threats.
- **Hu et al. [31]** utilized a CNN-GRU hybrid model applied directly to raw payload bytes. This model achieved a 98.2% F1 score on CIC-IDS2017, effectively capturing both local features (CNN) and temporal dependencies (GRU) within the payload. The training process for such hybrid models can be time-intensive, requiring substantial computational resources.
- **Ayantayo et al. [16]** implemented adversarial training on packet images using Fast Gradient Sign Method (FGSM) and Projected Gradient Descent (PGD) defenses. This approach maintained approximately 95% accuracy under adversarial conditions, demonstrating improved robustness against evasion attacks. However, adversarial training is computationally intensive, requiring significant resources for model development and deployment

4. Comparative Analysis of Flow-Based and Packet-Based NIDS

Flow-based and packet-based network intrusion detection systems (NIDS) have evolved significantly, each bringing distinctive capabilities tailored to various operational environments. Tables 1 and 2 summarize key studies from both domains, highlighting differences in architecture, datasets, strengths, and limitations.

Flow-based NIDS exhibit significant architectural diversity, ranging from GANs and ensemble models to attention-based and Bayesian networks. Commonly used datasets for evaluation include NSL-KDD, CIC-IDS2017, UNSW-NB15, and domain-specific datasets like IoTID20. Most studies report high AUC/F1 scores, particularly on benchmark datasets, with GANs and Bayesian models showing promise in zero-day or Out-of-Distribution (OOD) detection. Key trade-offs include increased model complexity for improved robustness (e.g., FlowGAN, UC-BNN), efficient class imbalance management with attention-based models, and the speed and explainability of feature selection frameworks, which may, however, overfit known patterns.

Table 1 presents a snapshot of recent flow-based approaches. These systems primarily leverage network flow metadata, offering lightweight and scalable detection suitable for high-throughput and encrypted environments. For instance, Li et al. [17] employed FlowGAN with strong zero-day detection capabilities (AUC ≈ 0.98), though at the cost of GAN training instability. Asadi et al. [22] combined CNN and LSTM to detect encrypted botnets with ~99.7% precision, yet remained vulnerable to adversarial perturbations like PGD and BIM. Robustness-enhancing methods, such as the ensemble attention model by Awad et al. [25], show promise but still exhibit similar vulnerabilities. Methods incorporating explainable or heuristic-driven learning (e.g., Emirmahmutoğlu & Atay [14], Khan et al. [28]) achieved high performance, F1-scores approaching 0.999, but lack adaptability to novel attack types.

In contrast, Table 2 summarizes packet-based NIDS, which analyze individual packet contents or their transformations (e.g., images or encoded sequences). These systems tend to demonstrate higher classification accuracy and adversarial robustness. Hore et al. [11] leveraged grayscale packet images and CNNs to reach 99.7% accuracy, while Nguyen et al. [13] applied transformer-based encoders to achieve near-perfect performance with strong generalization. Despite this, the computational cost of packet encoding, heavy preprocessing, and training time (e.g., Hu et al. [31]) remains a barrier to deployment in resource-constrained environments. Few-shot learning and augmentation-based strategies

(e.g., Verma et al. [30], Hore et al. [15]) show potential for zero-day detection but raise concerns about semantic drift and overfitting.

Packet-based NIDS excel in identifying fine-grained or low-volume attacks, including those embedded within encrypted traffic patterns and polymorphic payloads, due to their high data granularity. Architectural trends are dominated by CNNs, often paired with RNNs (GRU/LSTM) or transformers to capture both spatial and sequential patterns. Common data representations include image-based, byte sequence, and embedding-based encodings, with a growing trend towards multimodal input (e.g., combining header and payload information). While some works incorporate adversarial training or perturbation resistance, this area requires further research. Key challenges include high computational costs, large model sizes, and sensitivity to packet loss or capture noise, which can hinder real-time deployment.

Taken together, the comparison reveals that flow-based NIDS excel in efficiency, scalability, and deployment practicality, especially in scenarios with constrained computational budgets or encrypted traffic. Conversely, packet-based NIDS are better suited for precision-critical applications, offering stronger granularity, adversarial resilience, and deep feature representation, albeit with increased memory and runtime overhead. From a research perspective, this comparative survey provides a consolidated view of the trade-offs between flow-based and packet-based paradigms, offering readers a practical foundation for selecting architectures aligned with their constraints and threat models. For authors and system designers, the side-by-side analysis highlights key open challenges, such as the need for adaptive models, resilience against adversarial threats, and balanced computational demands. Moreover, this work encourages hybrid and context-aware designs that fuse the strengths of both categories, pointing toward an integrative roadmap for future NIDS research

Table 1 Summary of Flow-Based NIDS Approaches

Study (Year)	Data & Dataset	DL Architecture	Key Strengths	Drawbacks	Classification Type
Li et al. [17] (2024)	NSL-KDD, CIC-IDS, UNSW-NB15	Unsupervised FlowGAN	Strong zero-day detection (AUC ≈ 0.98)	GAN training instability	Binary (Normal vs. Anomalous Traffic)
Asadi et al. [22] (2025)	ISCX, ISOT	CNN + LSTM	~99.7% precision, scalable encrypted botnet detection	Vulnerable to PGD/BIM	Binary (Normal vs. Botnet Traffic)
Awad et al. [25] (2025)	CIC-IDS2017	Ensemble + Attention	Adversarially robust ensemble (≈ 95%)	Vulnerable to PGD/BIM	Binary (Normal vs. Intrusion)
Emirmahmutoğlu & Atay [14] (2025)	Multiple	Metaheuristic FS + ML	Near-perfect F1 (~0.999), explainable	Lacks zero-day adaptability	Binary (Normal vs. Abnormal)
Hu et al. [26] (2024)	CIC, NSL-KDD, KDD99	BiGRU + Self-Attention	~98.4% accuracy, handles class imbalance well	Higher runtime due to resampling	Binary (Normal vs. Attack)
Talpini et al. [27] (2024)	ToN-IoT [32-39], CIC	Bayesian NN + UQ	Reliable open-set detection	Slower inference	Multiclass (Network Traffic Classification into: DoS, Probe, R2L, U2R, and Normal)
Khan et al. [28] (2025)	IoTID20	ANN + GA	High IIoT accuracy (≈ 99.5%)	Hard to generalize beyond IIoT	Multiclass (Benign or Particular Intrusion Type) + Binary (Normal vs. Anomalous) and open-set classification

Table 2 Summary of Packet-Based NIDS Approaches

Study (Year)	Data & Dataset	DL Architecture	Key Strengths	Drawbacks	Classification Type
Hore et al. [11] (2024)	CIC-IDS2017	Grayscale Packet Images + CNN	99.7% accuracy, spatial insight	Heavy PCAP preprocessing	Multiclass classification (network intrusion detection, distinguishing between known attack patterns and novel/unseen samples)
Doriguzzi et al. [12] (2024)	UNSW/IDS2017	Multi-channel CNN + BiLSTM	~98% F1; temporal context captured	High encoding overhead	Binary classification (DDoS attack detection)
Nguyen et al. [13] (2025)	Multiple	Packet Transformer Encoder	~99% performance, robust	Memory-intensive	Binary classification (network intrusion detection - benign vs. malicious traffic, with adaptation to novel attack patterns)
Hore et al. [15] (2023)	Multiple	Augmented Packet Images + ResNet	Resilient to obfuscations	Risk of augmentation artifacts	Focuses on adversarial network packet generation to evade NIDS, implying a classification task (likely multiclass)
Verma et al. [30] (2025)	CIC + custom	Prototypical Few-Shot	Few data yet good performance	Issues with novel variants	Binary classification (anomaly-based intrusion detection - normal vs. abnormal)
Hu et al. [31] (2021)	CIC-IDS2017	CNN-GRU Hybrid	98.2% F1; sequential modeling	Long training time	Multiclass classification (network traffic classification into different applications, including encrypted ones)
Ayantayo et al. [16] (2023)	CIC & Bot-IoT[40-45]	FGSM/PGD-aware CNN	~95% robustness under attack	High training complexity	Multiclass classification (network intrusion detection)

As visualized in Figure 3, flow-based NIDS approaches report slightly higher average accuracy compared to packet-based ones, reflecting their maturity, scalability, and suitability for high-throughput environments, despite some trade-offs in adversarial robustness.

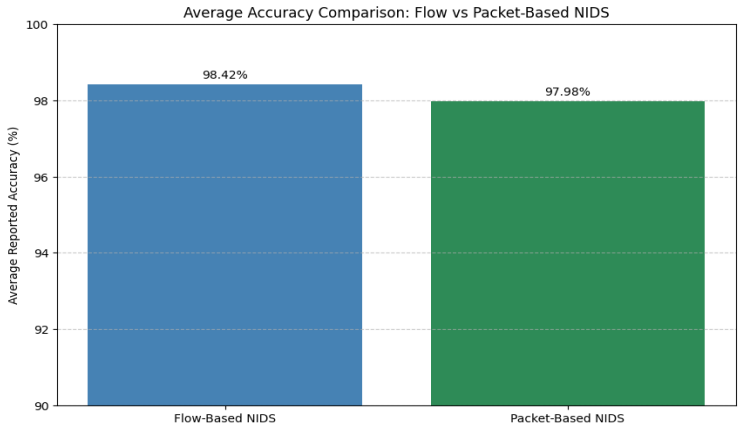


Figure 3. Average Accuracy Comparison: Flow vs Packet Based NIDS

5. Comparative Discussion of Datasets

The quality and characteristics of datasets play a pivotal role in shaping the performance and generalizability of NIDS. Throughout the reviewed studies, a diverse range of datasets has been employed: some legacy, some synthetic, and others designed for emerging domains like IoT or encrypted traffic. A comparative reflection reveals significant implications for benchmarking and reproducibility. NSL-KDD and KDD99 are among the earliest datasets used predominantly in flow-based studies (e.g., [17], [26]), valued for their simplicity and structured labeling. However, they suffer from outdated traffic profiles, limited protocol diversity, and lack of modern attack vectors—leading to models that risk overfitting or poor real-world translation. In contrast, CIC-IDS2017 has become a de facto standard across both flow-based (e.g., [25]) and packet-based approaches (e.g., [11], [31]). It offers full PCAPs with diverse benign and malicious behaviors, making it well-suited for packet-image conversion, deep sequence modeling, and botnet detection. Nevertheless, it includes time overlaps and imperfect labeling, which may bias temporal learning architectures. Datasets like UNSW-NB15 and ToN-IoT address some of these issues by incorporating modern protocol behaviors, IoT scenarios, and richer feature sets. Flow-based models such as [14] and [27] have leveraged them to assess generalizability in heterogeneous environments. However, preprocessing inconsistencies and the synthetic nature of attacks may still raise concerns about real-world fidelity. More specialized datasets like IoTID20, Bot-IoT, ISOT, and ISCX appear in studies focusing on IIoT, botnet detection, or encrypted traffic (e.g., [22], [28], [16]). These datasets offer valuable diversity in terms of device types, traffic encryption, and attack sophistication. Yet, they often lack labeling granularity and standard feature schemas, which challenge model interoperability. Overall, the dataset comparison underscores a fundamental tension between realism and control. Older datasets provide consistency but lack relevance, while newer ones offer realistic diversity at the cost of labeling accuracy or reproducibility. For future work, this suggests the need for benchmarking frameworks that integrate multi-dataset training and cross-dataset validation, ensuring robust, scalable, and unbiased NIDS evaluation pipelines. As shown in Table 3, datasets vary significantly in terms of realism, attack diversity, and support for packet-level analysis. While legacy datasets like KDD99 and NSL-KDD remain widely used, more recent collections such as CIC-IDS2017, ToN-IoT, and UNSW-NB15 provide better coverage of modern threats and richer packet-level information, making them preferable for contemporary NIDS evaluations. Table 3 summarizes widely used NIDS datasets by their structure, number of features, and purpose. While older datasets like KDD'99 and NSL-KDD are limited to feature vectors (CSV), more recent datasets such as CIC-IDS2017, ISCX, and Bot-IoT provide both PCAP traces and labeled

features, allowing researchers to pursue both flow-based and packet-based modeling. IoT-specific datasets (e.g., ToN-IoT, IoTID20) address modern IIoT threats but vary in raw trace availability.

Table 3 Comparison of Commonly Used Datasets in NIDS Research

Dataset	Year	Type	Format	Notable Use Cases	Number of Samples	Number of Features w/o Class Label (CSV)
NSL-KDD	2009	Simulated	CSV	Classic baseline; low complexity	125,973 (train), 22,544 (test)	41
KDD'99	1999	Simulated	CSV	Legacy; used for comparison only	4,898,431 (original train), 1,074,992 (distinct train)	41
CIC-IDS2017	2017	Realistic	PCAP + CSV	Widely used; broad attack types	~3,000,000	78
UNSW-NB15	2015	Hybrid	PCAP + CSV	Balanced attacks & benign data	2,540,044	47
ISCX	2012	Realistic	PCAP + CSV	Flow and time-based IDS research	>2,000,000 (traffic packets)	22
ISOT	2011	Realistic	PCAP	Botnet behavior detection	1,379,274	Depends on extraction (~80+)
Bot-IoT	2018	IoT-focused	PCAP + CSV	Ideal for IIoT and DDoS research	>72,000,000 (pcap), ~3,000,000 (5% sample)	~84
ToN-IoT	2020	IoT-focused	CSV (per source)	Lightweight IIoT NIDS evaluation	2,233,921	41
IoTID20	2020	IoT-focused	PCAP + CSV	IIoT attack fingerprinting	625,783	~81

6. Conclusion and Future Directions

In this survey, flow-based and packet-based deep learning approaches for Network Intrusion Detection Systems (NIDS) were reviewed and compared. Architectural characteristics, dataset preferences, detection capabilities, and vulnerabilities were analyzed to offer a holistic understanding of the current research landscape. Flow-based systems were generally observed to provide higher scalability and reduced computational overhead. These systems tend to be more efficient for encrypted or high-speed traffic scenarios. Conversely, packet-based approaches were often associated with higher detection accuracy for fine-grained threats, due to their ability to extract rich spatial and sequential features from raw packets. However, this came at the cost of increased preprocessing and memory consumption. Key findings from this survey may be summarized as follows:

- A lack of standardized benchmarking across studies was identified, which has made objective comparisons difficult. A shared evaluation protocol, supported by reproducible splits of public datasets, is recommended.
- Most existing approaches were found to operate exclusively on either flow or packet representations. The integration of both representations into hybrid models has been proposed by some studies but remains largely underutilized.

- Few models were observed to incorporate explainability or uncertainty quantification techniques. These features are increasingly important for deployment in critical or safety-sensitive environments.

To advance this domain, several research directions are suggested. Future work may focus on (1) the design of hybrid NIDS frameworks that dynamically adjust between flow and packet inputs based on context, (2) the development of lightweight yet explainable models for resource-constrained networks, and (3) the creation of new datasets that better reflect emerging attack vectors, such as those targeting IoT and encrypted communications.

References

1. Akande, Babatunde. (2025). AI-Enhanced Intrusion Detection Systems: Leveraging Data Structures for Scalable and Reliable Cybersecurity Solutions.
2. Ciancioso, Richard & Budhwa, Danvers & Hayajneh, Thaier. (2017). A Framework for Zero Day Exploit Detection and Containment.
3. Talukder, Md. Alamin & Islam, Manowarul & Uddin, Md Ashraf & Hasan, Fida & Sharmin, Selina & Alyami, Salem & Moni, Mohammad Ali. (2024). Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction. Journal of Big Data.
4. Mutambik, Ibrahim. (2024). An Efficient Flow-Based Anomaly Detection System for Enhanced Security in IoT Networks. Sensors.
5. Pinto, Andrea & Herrera, Luis-Carlos & Donoso, Yezid & Gutierrez, Jairo. (2023). Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure.
6. Mambwe Sydney, Kasongo. (2022). A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework. Computer Communications.
7. Yulianto, Semi & Soewito, Benfano & Gaol, Ford & Kurniawan, Aditya. (2024). Enhancing Cybersecurity Resilience through Advanced Red Teaming Exercises and MITRE ATT&CK Framework Integration: A Paradigm Shift in Cybersecurity Assessment. Cyber Security and Applications.
8. Cisco Systems. (2012). Introduction to Cisco IOS NetFlow. https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html
9. Boschi, E., Mark, L., & Claise, B. (2008). IP Flow Information Export (IPFIX) Applicability. RFC 5472. https://doi.org/10.17487/RFC5472
10. Phaal, P., Panchen, S., & McKee, N. (2001). sFlow Version 5 Specification. InMon Corp. https://sflow.org/sflow_version_5.txt
11. Hore, Soumyadeep & Ghadermazi, Jalal & Shah, Ankit & Bastian, Nathaniel. (2024). A sequential deep learning framework for a robust and resilient network intrusion detection system. Computers & Security.
12. Doriguzzi Corin, Roberto & Knob, Luis & Mendozzi, Luca & Siracusa, Domenico & Savi, Marco. (2024). Introducing packet-level analysis in programmable data planes to advance Network Intrusion Detection. Computer Networks.
13. Nguyen, Quoc & Hore, Soumyadeep & Shah, Ankit & Le, Trung & Bastian, Nathaniel. (2025). FedNIDS: A Federated Learning Framework for Packet-Based Network Intrusion Detection System. Digital Threats: Research and Practice.

14. Emirmahmutoğlu, Emre & Atay, Yılmaz. (2025). A feature selection-driven machine learning framework for anomaly-based intrusion detection systems. Peer-to-Peer Networking and Applications.
15. Hore, Soumyadeep & Ghadermazi, Jalal & Paudel, Diwas & Shah, Ankit & Das, Tapas & Bastian, Nathaniel. (2023). Deep PackGen: A Deep Reinforcement Learning Framework for Adversarial Network Packet Generation.
16. Ayantayo, Abiodun & Kaur, Amrit & Kour, Anit & Schmoor, Xavier & Shah, Fayyaz & Vickers, Ian & Kearney, Paul & Abdelsamea, Mohammed. (2023). Network intrusion detection using feature fusion with deep learning. Journal of Big Data.
17. Li, Zeyi & Wang, Pan & Wang, Zixuan. (2024). FlowGANAnomaly: Flow-Based Anomaly Network Intrusion Detection with Adversarial Learning. Chinese Journal of Electronics. 33. 58-71.
18. Tavallaee, Mahbod & Bagheri, Ebrahim & Lu, Wei & Ghorbani, Ali. (2009). A detailed analysis of the KDD CUP 99 data set. IEEE Symposium. Computational Intelligence for Security and Defense Applications, CISDA.
19. Sharafaldin, Iman & Habibi Lashkari, Arash & Ghorbani, Ali. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization.
20. Iman Sharafaldin, Arash Habibi Lashkari, Saqib Hakak, and Ali A. Ghorbani, "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy", IEEE 53rd International Carnahan Conference on Security Technology, Chennai, India, 2019.
21. Yin, Yuhua & Jang-Jaccard, Julian & Xu, Wen & Singh, Amardeep & Zhu, Jinting & Sabrina, Fariza & Kwak, Jin. (2023). IGRF-RFE: a hybrid feature selection method for MLP-based network intrusion detection on UNSW-NB15 dataset. Journal of Big Data.
22. Asadi, Mehdi & Heidari, Arash & Navimipour, Nima. (2025). A New Flow-Based Approach for Enhancing Botnet Detection Efficiency Using Convolutional Neural Networks and Long Short-Term Memory. Knowledge and Information Systems.
23. Shiravi, A., Shiravi, H., Tavallaee, M., & Ghorbani, A. A. (2012). Toward developing a systematic approach to generate benchmark datasets for intrusion detection. Computers & Security.
24. Saad, S., Traore, I., Ghorbani, A. A., Sayed, B., Zhao, D., Lu, W., & Hakimian, P. (2011). Detecting P2P botnets through network behavior analysis and machine learning. In Proceedings of the 9th Annual International Conference on Privacy, Security and Trust (PST).
25. Awad, Omer & Çevik, Mesut & Farhan, Hameed Mutlag. (2025). An enhanced attention and dilated convolution-based ensemble model for network intrusion detection system against adversarial evasion attacks. Peer-to-Peer Networking and Applications.
26. Hu, Zhanhui & Liu, Guangzhong & Li, Yanping & Zhuang, Siqing. (2024). SAGB: self-attention with gate and BiGRU network for intrusion detection. Complex & Intelligent Systems.
27. Talpini, J., Sartori, F. & Savi, M. Enhancing trustworthiness in ML-based network intrusion detection with uncertainty quantification. J Reliable Intell Environ.
28. Khan, Mohammad & Reshi, Aijaz & Shafi, Shabana & Aljubayri, Ibrahim. (2025). An adaptive hybrid framework for IIoT intrusion detection using neural networks and feature optimization using genetic algorithms. Discover Sustainability.
29. Ullah and Q. H. Mahmoud (2020). A Scheme for Generating a Dataset for Anomalous Activity Detection in IoT Networks. In Goutte, C. & Zhu, X. (Eds.), Advances in Artificial Intelligence – Canadian AI 2020, Lecture Notes in Computer Science, Vol. 12109, pp. 586–597. Springer, Cham.
30. Verma, Priyanka & O'Shea, Donna & Newe, Thomas & Mehta, Nakul & Bharot, Nitesh & Breslin, John. (2025). ABIDS-VEM: leveraging an equilibrium optimizer and data ramification in association with ensemble learning for anomaly-based intrusion detection system.

31. Hu, Feifei & Zhang, Situo & Lin, Xubin & Wu, Liu & Liao, Niandong & Song, Yanqi. (2021). Network Traffic Classification Model Based on Attention Mechanism and Spatiotemporal Features.
32. Moustafa, Nour. "A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets." Sustainable Cities and Society (2021): 102994. Public Access Here.
33. Booij, Tim M., Irina Chiscop, Erik Meeuwissen, Nour Moustafa, and Frank TH den Hartog. "ToN IoT-The role of heterogeneity and the need for standardization of features and attack types in IoT network intrusion datasets." IEEE Internet of Things Journal (2021). Public Access Here.
34. Alsaedi, Abdullah, Nour Moustafa, Zahir Tari, Abdun Mahmood, and Adnan Anwar. "TON_IoT telemetry dataset: a new generation dataset of IoT and IIoT for data-driven Intrusion Detection Systems." IEEE Access 8 (2020): 165130-165150.
35. Moustafa, Nour, M. Keshk, E. Debie and H. Janicke, "Federated TON_IoT Windows Datasets for Evaluating AI-Based Security Applications," 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2020, pp. 848-855, doi: 10.1109/TrustCom50675.2020.00114. Public Access Here.
36. Moustafa, Nour, M. Ahmed and S. Ahmed, "Data Analytics-Enabled Intrusion Detection: Evaluations of ToN_IoT Linux Datasets," 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2020, pp. 727-735, doi: 10.1109/TrustCom50675.2020.00100. Public Access Here.
37. Moustafa, Nour. "New Generations of Internet of Things Datasets for Cybersecurity Applications based Machine Learning: TON_IoT Datasets." Proceedings of the eResearch Australasia Conference, Brisbane, Australia. 2019.
38. Moustafa, Nour. "A systemic IoT-Fog-Cloud architecture for big-data analytics and cyber security systems: a review of fog computing." arXiv preprint arXiv:1906.01055 (2019).
39. Ashraf, Javed, Marwa Keshk, Nour Moustafa, Mohamed Abdel-Basset, Hasnat Khurshid, Asim D. Bakhshi, and Reham R. Mostafa. "IoTBoT-IDS: A Novel Statistical Learning-enabled Botnet Detection Framework for Protecting Networks of Smart Cities." Sustainable Cities and Society (2021): 103041.
40. Koroniotis, Nickolaos, Nour Moustafa, Elena Sitnikova, and Benjamin Turnbull. "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset." Future Generation Computer Systems 100 (2019): 779-796. Public Access Here.
41. Koroniotis, Nickolaos, Nour Moustafa, Elena Sitnikova, and Jill Slay. "Towards developing network forensic mechanism for botnet activities in the iot based on machine learning techniques." In International Conference on Mobile Networks and Management, pp. 30-44. Springer, Cham, 2017.
42. Koroniotis, Nickolaos, Nour Moustafa, and Elena Sitnikova. "A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework." Future Generation Computer Systems 110 (2020): 91-106.
43. Koroniotis, Nickolaos, and Nour Moustafa. "Enhancing network forensics with particle swarm and deep learning: The particle deep framework." arXiv preprint arXiv:2005.00722 (2020).
44. Koroniotis, Nickolaos, Nour Moustafa, Francesco Schiliro, Praveen Gauravaram, and Helge Janicke. "A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports." IEEE Access (2020).
45. Koroniotis, Nickolaos. "Designing an effective network forensic framework for the investigation of botnets in the Internet of Things." PhD diss., The University of New South Wales Australia, 2020.