UDC 004.732.056 **doi:** https://doi.org/10.20998/2522-9052.2026.2.11

Vadym Poltoratskyi[1], Svitlana Gavrylenko[1,2]

[1] National Technical University “Kharkiv Polytechnic Institute”, Kharkiv, Ukraine
[2] Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

THE EVOLUTION OF INTRUSION DETECTION SYSTEMS: A COMPREHENSIVE REVIEW OF MODERN DATASETS, DEEP LEARNING APPROACHES, AND ARCHITECTURAL CHALLENGES

Abstract. Intrusion Detection Systems (IDS) remain a critical component of cybersecurity. They are rapidly evolving to counter increasingly complex threats across various environments, such as the Internet of Things (IoT), the Industrial Internet of Things (IIoT), vehicular networks, and critical infrastructure. **The objective of this work** is a comprehensive analysis of the evolution of Intrusion Detection Systems (IDS) from 2020 to 2025. Grounded in contemporary research, it examines the integration of Machine Learning (ML), Deep Learning (DL), Federated Learning (FL), and novel hybrid techniques into IDS, summarizing advancements in their operational capabilities. Key trends include a significant shift toward deep learning architectures - specifically Transformers and Vision Transformers (ViT) - for enhanced pattern recognition. Additionally, the adoption of Federated Learning and fog computing-based systems is observed, aiming to preserve privacy and address challenges related to data decentralization and non-independent and identically distributed (Non-IID) data. Furthermore, there is growing emphasis on Explainable AI (XAI), attack lifecycle-based datasets, and model robustness against adversarial attacks. **The results obtained**. The review proposes a comprehensive multi-criteria classification of systems, enabling a thorough description and comparison of various solutions. The paper critically evaluates contemporary input datasets and conducts a comparative efficiency analysis of different intrusion detection methodologies. Analysis indicates that although algorithms achieve accuracy exceeding 98% on benchmark datasets, several critical challenges remain unresolved. These include class imbalance, the capability to detect novel and unknown threats, scalability in real-world operational environments, and ethical privacy concerns. **Conclusions.** This study addresses gaps in previous reviews by highlighting the lack of unified datasets, the need for model validation in real-world environments, and adaptive protection against zero-day attacks and encrypted traffic. It proposes a roadmap for the development of more robust, decentralized, and interpretable IDS.

Keywords: machine learning; intrusion detection systems; data classification; neural networks; deep learning; transformer models; data preprocessing; key performance indicators.

1. Introduction

In the era of rapid digitalization, ensuring the reliability and security of computer networks has become a critical prerequisite for the functioning of the global economy. Corporate infrastructures, cloud environments, and Internet of Things (IoT) ecosystems generate exponentially growing volumes of telemetry data, the monitoring of which is essential for cyber threat detection. However, the evolution of adversarial tactics and increasing data transmission speeds challenge the efficacy of traditional cyber defense approaches.

1.1. Global Threat Landscape and Limitations of Traditional Tools. An analysis of leading international reports indicates a qualitative shift in the nature of cyberattacks. According to the Verizon 2025 Data Breach Investigations Report (DBIR), the threat landscape has undergone a critical transformation. A key trend is the sharp increase in incidents categorized as "System Intrusion".

The proportion of these complex, multi-stage attacks rose from 36% in 2024 to 53% in 2025, becoming the dominant threat vector. This category significantly surpassed social engineering attacks and basic web application attacks. Such a shift indicates that adversaries are increasingly employing sophisticated techniques aimed at deep infrastructure penetration rather than merely targeting the perimeter.

The comparative dynamics of key cyber incident patterns confirm that traditional signature-based tools and basic firewalls are losing effectiveness against attacks masquerading as legitimate activity.

The situation is further complicated by the continuous increase in network bandwidth. In modern high-speed backbones, packet sampling methods are frequently employed to reduce hardware load. Technical studies show that even moderate sampling rates can result in a visibility loss of up to 50% regarding malicious flows - particularly short-lived attacks - creating critical "blind spots" for monitoring systems.

1.2. Research Relevance. The necessity of transitioning from static defense methods to adaptive systems based on Artificial Intelligence is corroborated by the response of the scientific community. The publication dynamics in the Web of Science and Scopus databases for the query "Intrusion Detection System" demonstrate a clear upward trend, reaching peak values in 2024-2025.

Despite significant progress, existing IDS face challenges regarding zero-day attacks, encrypted traffic, and scalability in decentralized environments. The integration of Machine Learning (ML), Deep Learning (DL), and privacy-preserving techniques such as Federated Learning (FL) addresses many of these limitations; however, issues regarding model generalization and interpretability remain unresolved.

As previous reviews were often restricted to narrow scopes, this review aims to systematize global shifts in IDS architecture.

The objective of this study is a comprehensive analysis of the evolution of Intrusion Detection Systems (IDS) from 2020 to 2025. The paper systematically categorizes key technological advancements, particularly the adoption of Deep Learning, Transformer

architectures, and Federated Learning. Special attention is devoted to Explainable AI (XAI) methods and the development of defense strategies based on the full cyberattack lifecycle.

To achieve this objective, we seek to answer the following questions:

1. How have IDS evolved, and how have attack detection approaches changed under the influence of AI and distributed computing?
2. What is the taxonomy of modern IDS?
3. Which modern datasets are used for benchmarking, and what is their relevance and effectiveness?
4. How effective are emerging systems within specific domains?
5. What are the current performance metrics, operational constraints, and reliability criteria for IDS?
6. What characterizes the practical deployment of Intrusion Detection Systems?
7. Which problems remain unresolved?

1.3 Review Stages and Methodology. This paper covers peer-reviewed research published between 2020 and 2025. The review was conducted in accordance with the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) international standard, ensuring transparency and objectivity in the selection process.

The research process comprised three stages:

1. Selection of publications based on keywords related to ML, DL, FL, and IoT.
2. Analysis of the relevance and quality of the selected articles.
3. Systematization of the obtained results and identification of promising defense methods.

2. Historical Evolution of Intrusion Detection Systems

2.1 Brief Historical Overview. The conceptual foundations of intrusion detection were established in the early 1980s. The technical report Computer Security Threat Monitoring and Surveillance (1980) by James P. Anderson [1], prepared for the United States Air Force, is regarded as the historical cornerstone of the field. Anderson was the first to propose utilizing computer system audit logs not merely for accounting but for automated threat detection, introducing the classic taxonomy of intruders: external penetrators, masqueraders, and misfeasors.

The theoretical and mathematical foundations of the field were established by Dorothy E. Denning [2]. In her seminal work "An Intrusion-Detection Model", published in IEEE Transactions on Software Engineering (February 1987), she formalized the first real-time intrusion detection model. Denning hypothesized that any malicious activity manifests as a deviation from normal system usage patterns and proposed a structure of profiles to quantify such anomalous behavior.

These theoretical advancements laid the groundwork for early practical implementations. Systems such as the Intrusion Detection Expert System (IDES), developed at SRI International in the late 1980s, and the Network Security Monitor (NSM) in the 1990s, integrated Denning's statistical models with expert rules, analyzing both system logs and network traffic.

The period of the 1990s and 2000s was marked by the dominance of signature-based detection systems. A prime example of this era was the emergence of Snort in 1998, developed by Martin Roesch. Due to high-efficiency pattern matching mechanisms, such systems became the industry standard for blocking known attacks. However, the rapid proliferation of new threats and polymorphic viruses quickly exposed the primary deficiency of the signature-based approach: the inability to counter zero-day attacks.

The integration of Machine Learning (ML) in the early 2000s emerged as a response to the need for adaptability. Researchers began applying Decision Trees, Support Vector Machines (SVM), and early Neural Networks. A significant, albeit controversial, catalyst for this period was the release of the KDD Cup 1999 dataset. It enabled the standardization of experiments, although it later faced valid criticism regarding outdated attack models and the artificial nature of the traffic.

Since 2010, the explosive growth of Big Data, the proliferation of cloud computing, and Internet of Things (IoT) ecosystems have driven the transition to Deep Learning (DL) methods. The capability of neural networks to automatically extract features from "raw" high-dimensional data has significantly improved detection accuracy in complex networks.

2.2 The Modern Stage of IDS Development. The modern stage (2020-2025) is characterized by a transition toward privacy-centric intelligent ecosystems.

Since 2020, scholarly literature has demonstrated a distinct emphasis on the application of Machine Learning (ML) [3, 4] and Deep Learning (DL) [5] for securing specific environments, such as the Internet of Things (IoT) and vehicular networks. Specifically, Asharf et al. [6] analyzed architectures and threats within IoT ecosystems, highlighting the critical need for lightweight models capable of operating on low-power devices despite the poor quality of available data. Expanding on this theme, Khraisat and Alazab [7] proposed a comprehensive taxonomy of IDS for IoT, devoting particular attention to sensor placement strategies and the significance of utilizing dynamic traffic features for precise attack detection.

Concurrently, Seyfollahi and Ghaffari [8] investigated a narrower domain: vulnerabilities within the RPL protocol, the standard for Low-Power and Lossy Networks (LLNs). The authors concluded that efficient defense in resource-constrained environments requires the development of complementary lightweight detection mechanisms.

Subsequent studies expanded the scope of the field, shifting from general surveys to the analysis of highly specialized methods and large-scale meta-analyses. Specifically, Stavroula et al. [9] explored the capabilities of Generative Adversarial Networks (GANs) for synthetic data generation. They demonstrated that these neural networks effectively facilitate dataset balancing by augmenting instances of rare attacks. However, the researchers highlighted that GAN performance remains suboptimal in processing discrete traffic features.

In parallel, Rabbani et al. [10] developed a classification of Machine Learning methods for detecting malicious behavior in emerging environments: Cloud and Fog computing. The authors emphasized that the primary barriers remain the low quality of training data and the complexity of scaling systems to large-scale networks.

Issues regarding privacy and data exchange were examined in detail by Agrawal et al. [11], who analyzed the potential of Federated Learning (FL). While describing the fundamental architectures of this approach, they also identified significant challenges: the complexity of handling heterogeneous data across diverse devices (the Non-IID problem) and the high communication overhead during model synchronization.

Recent scientific works encompass an even broader spectrum of technologies and offer a more thorough evaluation of existing methods [12]. Notably, Ziadoon K. et al. [13] conducted a large-scale analysis of research dedicated to network anomaly detection systems. Their work confirmed a global trend: Deep Learning (DL) currently dominates the field, accounting for 50% of all developments, while classical Machine Learning constitutes only 30%. Although such systems demonstrate exceptionally high accuracy, the authors emphasize that the problem of data imbalance remains unresolved. This view is supported by Genuario et al. [14], who, in their analysis of methods, demonstrated that the best results today are yielded by ensemble approaches, which combine multiple algorithms into a single system.

The issue of data quality became central in the work of Akbar K. et al. [15]. After analyzing 37 datasets, the authors concluded that none are perfect and proposed a framework for unified data selection.

In parallel with the pursuit of universal solutions, highly specialized research directions are actively advancing. For instance, Verma et al. [16] introduced the ROAD dataset for Intrusion Detection Systems in Controller Area Networks (CAN). This contribution addressed the scarcity of realistic data for vehicular networks.

The majority of specialized reviews in 2025 focus on system adaptability and data privacy. Fteiha et al. [17] analyzed the adaptability of IDS to dynamic changes within Internet of Things (IoT) environments. The authors concluded that superior results are achieved through hybrid methods that combine the strengths of various detection algorithms [18]. Finistrella et al. [19] systematized solutions based on Reinforcement Learning (RL), with a specific focus on Multi-Agent Reinforcement Learning (MARL) systems for more coordinated defense mechanisms.

The security issues intrinsic to distributed systems themselves were addressed by Latif et al. [20]. In their investigation of Federated Learning, they identified specific threats, such as data poisoning attacks. These attacks involve the injection of malicious samples into the training process to surreptitiously compromise the model. Despite these risks, the researchers also highlighted the high effectiveness of hybrid models in mitigating such threats.

Notwithstanding their scientific value, the majority of the aforementioned works share a common limitation: a narrow scope. For instance, the studies by Finistrella (MARL), Verma (CAN), and Bourou (GAN) provide in-depth explorations of specific topics but fail to integrate these methodologies into a unified system.

A similar situation is observed in reviews dedicated to specific environments, such as IoT [6] or Host-based Intrusion Detection Systems (HIDS) [21]. By focusing exclusively on the specifics of their respective domains, these works often overlook the potential for broader result generalization. Other researchers examine highly specialized problems in detail yet fail to conduct a systematic analysis that would facilitate the cross-domain transfer of successful methodologies.

Key trends in the modern stage of IDS development include the adoption of Transformer architectures for traffic sequence analysis, the advancement of Federated Learning (FL) for privacy preservation, and the integration of Explainable AI (XAI) methods [22]. These technologies enable effective mitigation of dynamic threats in decentralized environments, ensuring a balance between security and user privacy.

However, the review indicated that the majority of studies remain narrowly specialized, necessitating their integration into a unified system.

In contrast to narrowly focused reviews, this work proposes a unified comprehensive taxonomy, a detailed analysis of datasets, and a comparative evaluation of method efficiency across various domains. The study places central emphasis on critical yet frequently overlooked issues:

- practical deployment of systems in real-world environments;
- model robustness against adversarial attacks;
- handling of dynamic data;
- efficient scalability of distributed systems.

3. IDS Taxonomy

The classification of Intrusion Detection Systems (IDS) is conducted across multiple dimensions, a process that is crucial for selecting the optimal architecture for specific operational environments. The proposed taxonomy is grounded in an analysis of contemporary literature and extends traditional categories by integrating emerging trends: hybrid approaches, decentralized models, and specialized domain-specific solutions (Fig. 1).

3.1 Threat Detection Approaches. Based on the threat analysis methodology, IDS are categorized into three primary classes: signature-based, anomaly-based, and hybrid.

Signature-based systems perform traffic matching against a database of known attack patterns. Their primary advantage is a low false positive rate (FPR) when detecting established threats; however, they remain ineffective against zero-day attacks [23].

Anomaly-based systems model a baseline of normal system behavior and flag any deviations as potential threats. This capability enables the detection of novel attack types but frequently results in an elevated false positive rate [24, 25].

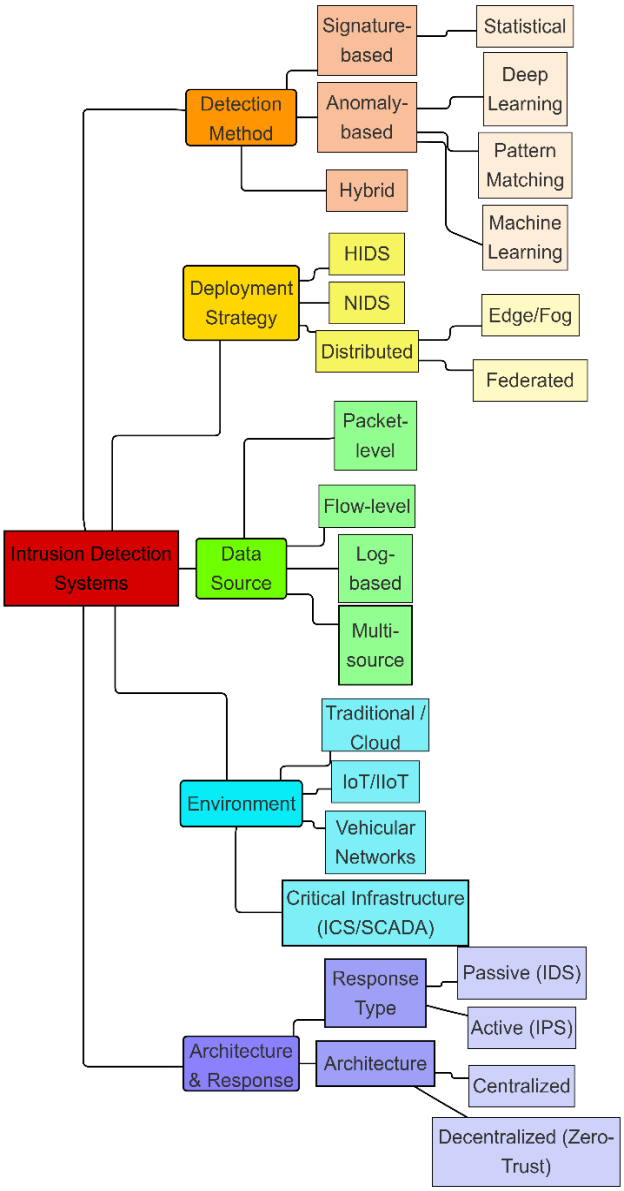

Fig. 1. Proposed classification of Intrusion Detection Systems integrating traditional approaches with emerging paradigms and domain-specific environments

Hybrid approaches integrate both methods to achieve a balance between detection precision and recall. A prominent example is the hybrid system proposed by Sajad E. et al. [26]. It combines neural networks for signature generation with fuzzy logic for anomaly detection, achieving an accuracy of 96.11%. Conversely, Feng L. et al. [27] developed a multi-layered hybrid system for SOME/IP vehicular networks. It integrates rule-based header analysis with Multi-GRU (Gated Recurrent Unit) for payload anomaly detection, demonstrating high accuracy.

3.2 Deployment Strategy. Depending on the deployment location within the infrastructure, IDS are classified into Host-based (HIDS), Network-based (NIDS), and Distributed systems.

Host-based IDS (HIDS) monitor individual endpoints through the analysis of event logs and system calls. They provide deep incident granularity but possess limited scalability.

Network-based IDS (NIDS) analyze traffic across the entire network. This ensures broad infrastructure visibility; however, such systems may miss threats within encrypted traffic or local attacks occurring inside a node.

Distributed and Edge deployments address latency issues in IoT and Fog computing environments.

For example, Rocha et al. [28] introduced DCIDS, a distributed host-based system (HIDS) for Kubernetes containerized environments, which achieved an anomaly detection accuracy exceeding 99%. Hybrid deployments, such as the integration of Suricata for network monitoring in the work by Sajad E. et al. [26], allow for striking a balance between network coverage and computational overhead.

3.3 Data Source and Environment. The effectiveness of IDS is contingent upon the type of input data, which may include packets, flows, event logs, system calls, or a combination thereof. Environments range from traditional corporate networks to specialized domains: IoT, IIoT, vehicular networks, and SCADA.

Packet-level analysis (Deep Packet Inspection, or DPI) is suitable for high-precision detection, whereas flow-level analysis ensures higher throughput. In the aforementioned studies, Feng L. et al. [27] utilized packet data for securing vehicular networks, while Rocha et al. [28] focused on system calls within containers. It is worth noting that emerging environments require resource-efficient (lightweight) and adaptive architectures.

3.4 Architecture and Level of Autonomy. This section of the taxonomy integrates two critical parameters defining the operational model of IDS: the response mechanism and the data processing topology.

In the context of the level of autonomy, the spectrum of solutions has evolved from classic passive IDS, restricted to monitoring and alerting, to modern Intrusion Prevention Systems (IPS) and Security Orchestration, Automation, and Response (SOAR) platforms.

The latter are capable of not only detecting but also dynamically isolating threats in real-time without human intervention.

Regarding architecture, a distinct shift is observed from monolithic centralized solutions to decentralized models. A prominent example is the implementation of Federated Learning (FL) frameworks, which enable model training on edge devices without the necessity of transmitting "raw" data to a central server. This comprehensive classification underscores the transformation of the field toward the development of hybrid, distributed, and adaptive systems, which is critically important for resource-constrained environments with elevated privacy requirements.

4. Datasets for IDS Evaluation

The quality, relevance, and representativeness of training data serve as the foundation upon which the effectiveness of any modern Intrusion Detection System is built. In the era of Machine and Deep Learning, a dataset ceases to be merely an archive of network packets, transforming into a critical component of the security architecture that determines the model's

generalization capability. This section analyzes the evolution of benchmark databases, highlights the methodological challenges in their construction, and examines modern resources that meet the demands of emerging threats.

4.1 Challenges in Data Formation and Validation. Traditional datasets, such as KDD99 and NSL-KDD, served as the benchmark for academic research for a long time; however, today they are subject to valid criticism due to outdated attack vectors, the synthetic nature of the traffic, and a lack of realism, rendering them unsuitable for training modern neural networks. Modern researchers face a complex set of challenges, dominated by the problem of class imbalance: in real-world traffic, the proportion of normal activity significantly exceeds the number of attacks [29, 30]. This complicates model training, leading to bias toward the majority class and reduced detection accuracy for rare threats.

The situation is exacerbated by the insufficient diversity of existing samples and the weak representation of emerging threats, specifically zero-day attacks, adversarial examples, and domain-specific exploits. This causes a generalization problem, where models, having demonstrated high efficiency in a test environment, prove ineffective when deployed in a real network with a different topology or traffic profile. Additional barriers include strict privacy constraints, which preclude the publication of data from real deployed systems, and the need for dynamic scenarios that reflect the full lifecycle of a cyberattack (Cyber Kill Chain).

In response to these challenges, a critical requirement for modern datasets is their alignment with the MITRE ATT&CK matrix. This global knowledge base systematizes cyber threat tactics and techniques based on real-world observations, focusing not on static signatures but on attacker behavior (tactical goals and technical methods of achievement). Utilizing MITRE ATT&CK allows for training systems to recognize intrusion logic at various stages of its progression, rather than merely recording isolated incidents.

Recent reviews, notably Akbar K. et al. [15], highlight the absence of a universal dataset that satisfies all these criteria, creating a persistent demand for authentic and current benchmarking solutions.

4.2 Overview of Modern Datasets (2020-2025). Datasets developed during the 2020-2025 period are characterized by a shift from abstract simulations to the capture of traffic within real physical environments.

In the domain of automotive security, a significant contribution was the introduction of the ROAD dataset, which contains recordings of real attacks on the Controller Area Network (CAN) bus of a physical vehicle, including fuzzing, fabrication, and masquerade attacks. Of particular value is the preservation of signal translation, which enables the detection of stealthy attacks that do not disrupt timing characteristics. To ensure evaluation objectivity within this same domain, Brooke L. and Weizhi M. [31] introduced Can-train-and-test, a specialized resource with a distinct separation between training and testing splits, addressing the issue of "data leakage" during model training.

Significant progress is observed in the creation of resources for the Internet of Things (IoT) and Edge computing. A comprehensive approach was demonstrated by Ferrag et al. [32] in the Edge-IIoT-2022 dataset, which encompasses diverse attack scenarios for testing multi-class classification within a 7-layer architecture. For real-time applications, Sharmila et al. [33] developed RT-IoT2022, which accounts for non-parametric traffic distributions of operational infrastructure. Research scalability was facilitated by CICIoT2023 Kazi F. et al., [34], which, due to its substantial data volume, enables effective modeling of Federated Learning scenarios and the investigation of model interpretability.

In parallel, highly specialized solutions for critical sectors are evolving. In the healthcare domain, Dadkhan et al. [35] introduced CICIoMT2024, which incorporates threats specific to the Internet of Medical Things (IoMT) network. For critical infrastructure protection, researchers focused on industrial protocols: Arifin et al. [36] developed a dataset for the IEC 60870-5-104 protocol in SCADA systems, and Dehlaghi-Ghadim et al. [37] created ICS-Flow for flow analysis in industrial control systems. Energy grid security is addressed in the UNSW-MG24 dataset [38] for microgrids and the ORNL dataset [39] for power systems.

Beyond domain-specific characteristics, new datasets address fundamental methodological challenges. Didik S. et al. [40] introduced the unique CREMEv2 dataset, constructed based on the full attack lifecycle (MITRE ATT&CK), which facilitates the analysis of sequential attacker behavior.

The issue of class imbalance in network traffic is addressed in Maple-IDS [41], while the challenges of analyzing encrypted traffic (specifically DNS-over-HTTPS) are resolved by CIRA-CIC-DoHBrw-2020 [42]. Additionally, TII-SSRC-23 [43] is utilized for the general analysis of diverse traffic.

4.3 Comparative Analysis of Trends. The conducted analysis of modern datasets (Table 1) enables the identification of key evolutionary vectors in IDS benchmarking. Unlike previous generations, modern solutions are shifting away from universality in favor of deep specialization. This manifests as a distinct transition from capturing simple volumetric threats (DoS/DDoS), which dominated early datasets, to modeling complex stealthy behavior, such as masquerade attacks in the ROAD dataset or multi-stage intrusion chains in CREMEv2.

Concurrently, the analysis reveals systemic issues. Despite the increase in realism, datasets such as Edge-IIoT-2022 and CICIoMT2024 are still characterized by substantial class imbalance, creating a risk of AI model bias. A positive trend is that the newest datasets (specifically CICIoT2023) incorporate the requirements of emerging architectures - Federated Learning and Explainable AI (XAI) - during the design phase.

In summary, while the examined datasets demonstrate significant progress in modeling realistic scenarios, none currently fully address the challenges of dynamic data updates and the comprehensive coverage of adversarial attacks.

Table 1 – **Comparison of selected modern IDS datasets (2020–2025)**

Dataset (Year)	Environment & Source	Format & Volume	Features	Protocols	Balance (Normal: Attack)	Attack Classes
ROAD (2021)	Automotive. Real vehicle (physical testbed), signal masking.	Log/Signal. ~3.5 hours of recording.	11 features	CAN	~5 : 1 (Balanced in fragments)	3 types: Fuzzing, Fabrication, Masquerade (hard to detect).
Edge-IIoT-2022 (2022)	IIoT/Edge. 7-layer testbed (Cloud, Fog, Edge, IoT). Real sensors.	CSV + PCAP. ~20 million records (20.9 GB).	61 features	MQTT, Modbus, CoAP, HTTP, ZigBee	~1:1 (Highly balanced)	14 types: (DoS/DDoS, MITM, Injection, Malware, Scanning).
CICIoT2023 (2023)	General IoT. 105 IoT devices, real network topology.	CSV + PCAP. ~46 million records (massive).	47 features	TCP/UDP, HTTP, MQTT	Extremely unbalanced (Attacks dominate due to DDoS)	33 types: (7 categories, focus on Mirai/Botnets).
CICIoMT2024 (2024)	IoMT. 40 devices (Wi-Fi, Bluetooth, MQTT). Real + simulated.	CSV + PCAP. ~8.8 million records.	45 features	MQTT, TCP, UDP, Bluetooth, Wi-Fi	~1:37 (Extreme imbalance: only 2.6% normal vs 97.4% attacks)	18 scenarios in 5 categories: DDoS, DoS, Recon, MQTT attacks, Spoofing.
CREMEv2 (2023)	Enterprise. Full attack lifecycle emulation (Kill Chain).	PCAP + Logs. ~30 GB (12 scenarios).	Raw data	HTTP, FTP, SSH, DNS	High imbalance (Attacks < 1%)	MITRE ATT&CK: (Recon → Exploit → Lateral Movement).
RT-IoT2022 (2022)	Real-Time IoT. Hybrid testbed: real devices + emulated attacks.	CSV. ~161k records (small).	83 features	MQTT, ThingSpeak, HTTP, DNS	Unbalanced (Attacks exceed normal ~7:1)	12 types: (DoS, Brute Force, MQTT attacks, Port Scanning, Spoofing).

5. Analysis of Key Methodologies in Modern Intrusion Detection Systems

This section presents a detailed analysis of the primary methodologies employed in modern Intrusion Detection Systems (IDS). They are categorized into statistical and traditional Machine Learning approaches, Deep Learning-based methods, as well as hybrid and emerging techniques.

The analysis is grounded in current research and evaluates architectural innovations, feature processing strategies, performance metrics, and existing limitations. The review illustrates the gradual evolution of the field toward the creation of more adaptive, efficient, and privacy-centric architectures suitable for complex environments such as IoT, IIoT, vehicular networks, and cloud infrastructures.

To facilitate comparison, key performance metrics from the studied works are summarized in the tables below (Tables 2–4).

5.1 Statistical and Traditional Machine Learning Approaches. Statistical methods and traditional Machine Learning (ML) remain the foundation of IDS due to the interpretability of their decision logic, low computational resource requirements, and high efficiency on structured data. These methods typically encompass supervised learning algorithms [44], ensemble methods [45], and statistical anomaly analysis [23]. Their efficiency is frequently enhanced through dimensionality reduction, feature selection, and class balancing techniques, rendering them robust when processing high-dimensional network data.

A significant trend is the utilization of sophisticated feature selection methods to overcome the "curse of dimensionality." For instance, Eljialy et al. [46] developed a comprehensive framework integrating ANOVA, correlation analysis, mutual information, and other statistical tests. By employing an XGBoost classifier on the SDN-IoT dataset, they achieved an accuracy of 99.0% with only 17 selected features, demonstrating effective dimensionality reduction without compromising performance.

Ensemble learning further enhances detection capabilities [47, 48]. Ali, M. et al. [49] proposed a stacking ensemble utilizing KNN, SVM, and Random Forest (RF) as base models, with XGBoost serving as the meta-classifier. On the CIPMAIDS2023-1 dataset, they achieved an F1-score of 98.24%. However, validation on a different dataset (CICIDS2017) revealed an accuracy drop to ~78%, highlighting the generalization problem inherent in these models.

Amit S. et al. [50], utilizing the CICIDS2018 dataset, compared ten algorithms, including AdaBoost, MultinomialNB, Decision Tree, GaussianNB, KNN, Logistic Regression, Random Forest, SGD, SVM, and XGBoost. The application of SMOTETomek and RandomOverSampler balancing methods enabled XGBoost to achieve 99.30% accuracy in multi-class classification, while KNN demonstrated 99.49% in binary classification. This confirms the value of oversampling for detecting zero-day attacks and indicates the necessity of testing robustness against adversarial threats.

Effective statistical methods also address the challenge of real-time operation. Josy V. and Balachandra M. [51] introduced the D3 framework for securing SDN (Software-Defined Networking) against DDoS attacks. The utilization of DPDK technology and a weighted moving average method enabled a reduction in CPU load to 0.02% while maintaining an accuracy of 96.59%.

Domain-specific adaptations include non-parametric approaches. Sharmila et al. [33] confirmed the effectiveness of statistical tests on the RT-IoT2022 dataset, achieving an accuracy of 99.85% using Decision Trees. In the realm of Industrial Internet of Things (IIoT),

Thi-Thu-Huong L. et al. [52] and Doghramachi D. and Siddeeq A. [53] successfully applied XGBoost with class imbalance handling techniques, obtaining near-perfect accuracy (>99.8%).

In summary, traditional ML excels in efficiency and transparency but necessitates rigorous Feature Engineering and possesses limitations when processing "raw" sequential data.

Table 2 – **Performance metrics for selected traditional ML approaches**

Study	Model / Architecture	Dataset	Accuracy (%) (Binary / Multi)	Optimization Technique (Methodology)	Key Contribution / Result
Eljialy et al. [46]	XGBoost	SDN-IoT	99.00 (B)	Feature selection (ANOVA, Correlation, Mutual Info, Chi-square), PCA	Data dimensionality reduction for enhanced efficiency in SDN.
Ali et al. [49]	Stacking Ensemble	CIPMAIDS2023	98.24 (M) (Average F1)	Multi-level stacking (KNN, SVM, RF + XGBoost)	Accuracy improvement, but generalization issues across datasets revealed.
Amit S. et al. [50]	XGBoost / KNN	CICIDS2018	99.49 (B) 99.30 (M)	Hybrid resampling (SMOTETomek)	Effective detection of zero-day attacks under severe imbalance conditions.
Sura E. et al. [54]	Voting Ensemble	CSE-CIC-IDS2018	98.82 (M)	Voting-based ensemble (DT, ExtraTrees, LR)	Reduction of model training time by 73% without accuracy loss.
Thi-Thu-Huong L. et al. [52]	XGBoost	TON_IoT X-IIoTID	99.90 (M) / 99.87 (M) (Average F1)	Specialized IIoT feature processing	Confirmation of Gradient Boosting superiority for industrial protocols.
Doghramachi D., Siddeeq A. [53]	XGBoost	IoTID20	99.00 (B/M)	Synthetic data generation (SMOTE)	Improved detection of rare attack subclasses in IoT.
Mhamad B. et al. [55]	Optimized RF	UNSW-NB15 CIC-DDoS2019	98.00 - 99.97 (B/M)	Feature Selection via GOA-GA algorithm	Creation of a hybrid tuning mechanism to maximize accuracy.
Aldabash, O. et al. [56]	Weighted RF	NSL-KDD CICIDS2017	99.92 (B) / 98 (B)	OWSA (Feature Selection) + ANN-Weighted RF	Addressing model bias toward normal traffic.
Sharmila et al. [33]	Decision Trees	RT-IoT2022	99.85 (B)	Non-parametric statistical tests	Statistical justification of feature selection for real-time systems.
Wenfeng, X. and Yongxian, F. [57]	LogAE + XGBoost	CICIDS2017	99.92 (M)	Logarithmic Autoencoder (LogAE)	Feature Enhancement.
Al Nuaimi et al. [58]	PART / J48	Edge-IIoT-2022	99.55 (B) 92.92 (M)	Rule-based algorithms	Priority of model interpretability over "black boxes" (DL).

5.2 Deep Learning-Based Approaches. Deep Learning (DL) methodologies have revolutionized IDS by enabling automated feature extraction directly from "raw" data. This capability allows for the detection of complex non-linear dependencies that are frequently overlooked by traditional methods.

5.2.1 Sequential Models and Transformers. In the realm of analyzing sequential network traffic data, recurrent architectures have long been dominant and are continuously being refined to handle complex threats. Specifically, Ridha H. S. et al. [59] successfully integrated LSTM networks with the SMOTE technique and feature selection algorithms. This approach allowed them to outperform baseline models on benchmark datasets CICIDS2017, NSL-KDD, and UNSW-NB15, effectively detecting minority attack classes despite the method's high computational intensity.

In parallel, approaches based on Deep Belief Networks (DBN) are advancing: Belarbi et al. [60] applied DBN with class balancing on CICIDS2017, which significantly improved the detection of rare attack types compared to classic Multi-Layer Perceptrons (MLP).

A significant step was the integration of attention mechanisms into traditional architectures: Alshehri et al. [61] introduced the SA-DCNN model for the Industrial Internet of Things (IIoT). In this model, the use of Self-Attention for dynamic feature weighting, combined with two-stage data cleaning, enabled it to outperform existing ML/DL counterparts on the IoTID20 and Edge-IIoTset datasets. The emergence of Transformer architectures marked a paradigm shift due to their capability for parallel data processing and capturing long-term dependencies in traffic [62]. Long et al. [63] proposed a Transformer-based NIDS for cloud environments, which achieved an accuracy exceeding 93%, demonstrating a lower false positive rate compared to CNN-LSTM hybrids.

In the IoT domain, Safi U. et al. [64] developed the TNN-IDS model for the MQTT protocol. By utilizing a multi-head attention mechanism and entropy-based feature selection, they achieved an impressive accuracy of 99.99% on the MQTT-IoT-IDS2020 dataset, significantly outperforming Recurrent Neural Networks (RNN).

The application of Transformers has also expanded to vehicular networks: Hyunjun, J. and Deok-Hwan, K. [65] adapted this architecture for analyzing CAN protocol traffic, achieving an F1-score of up to 99.8% with low classification latency. Of particular note is the work by Ghadermazi et al. [66], who introduced GTAE-IDS - a graph-transformer autoencoder that employs unsupervised learning and is capable of detecting anomalies from the very first packets, demonstrating an accuracy of over 98% on CIC-IDS2017.

Modern research also focuses on the creation of complex hybrid models and specialized integrations to further enhance performance. Safi U. et al. [67] combined LSTM and GRU architectures for the Internet of Vehicles (IoV), achieving up to 99.9% accuracy with minimal latency. A similar strategy was adopted by Benahmed et al. [68], who integrated Bidirectional LSTM (BiLSTM) with Deep Neural Networks (DNN) for the Internet of Medical Things (IoMT), obtaining an accuracy of 98.81%, although the authors noted the model's sensitivity to data imbalance.

Among other specialized solutions, the integration of ResNet with the CBAM (Convolutional Block Attention Module) attention mechanism in the work by Li et al. [41] on the Maple-IDS dataset (99.83%) is worth highlighting, as well as the simplified LSTM model by Sandeepkumar R. et al. [69], which ensures a balance between accuracy (97.67%) and energy efficiency for IoT devices.

5.2.2 Graph and Visual Transformer Approaches. Alternative data representation methods enable overcoming the limitations of traditional formats, such as tabular or simple sequential data, by capturing latent dependencies within traffic.

Zaccagnino et al. [70] proposed modeling network traffic in the form of graphs, utilizing Graph Neural Networks (GNN). They approached the intrusion detection task as a graph node classification problem. Due to the model's capability to account for structural and topological relationships between hosts, the authors achieved flawless attack detection on the UNSW-NB15 dataset.

An innovative trend involves the transformation of network traffic into visual representations to employ Computer Vision algorithms. Hai, Z. et al. [71] developed the HiViT-IDS model, which converts network flows into RGB images for subsequent processing by a Vision Transformer (ViT). This approach demonstrated near-perfect accuracy on the Edge-IIoTset dataset. Notably, the training of this model was 3.6 times faster than that of Convolutional Neural Networks (CNN) on the ToN-IoT dataset, attesting to the high efficiency of Transformers.

Deep Learning (DL) methods consistently demonstrate State-of-the-Art (SOTA) accuracy across diverse datasets. However, their implementation demands significant computational resources and rigorous regularization to prevent overfitting, particularly on small or imbalanced samples.

Table 3 – **Performance metrics for selected Deep Learning approaches**

Study	Model / Architecture	Dataset	Accuracy (%) (Binary/Multi)	Optimization Technique (Methodology)	Key Contribution / Result
Long et al. [63]	Transformer	Cloud Datasets	>93.00 (M)	Attention Mechanisms	Reduction of False Positive Rate (FPR) compared to CNN-LSTM hybrids.
Safi U. et al. [64]	TNN-IDS (Transformer)	MQTT-IoT-IDS2020	99.99 (M)	Multi-Head Attention, parallel processing	Highly effective protection of the specific MQTT protocol in IoT.
Hyunjun, J., Deok Hwan, K. [65]	Transformer	Car Hacking (CAN)	99.80 (M)(F1)	Adaptation for Time-Series	Provision of Low Latency, critical for automotive transport.
Ghadermazi et al. [66]	Graph-Transformer AE	CIC-IDS2017	>98.00 (B)	Unsupervised Learning	Ability to detect anomalies from the very first connection packets.
Hai, Z. et al. [71]	HiViT-IDS (Vision ViT)	Edge-IIoTset ToN-IoT	100.00 (M) 99.7 (M)	Traffic-to-Image conversion	Acceleration of model training by 3.6 times compared to CNN.
Zaccagnino et al. [70]	GNN (Graph Network)	UNSW-NB15	~100.00 (B)	Flow similarity graph (Nodes = Traffic Samples)	Use of shared features (Protocol, State) to construct an anomaly graph.
Li Q. et al. [41]	ResNet + CBAM	Maple-IDS	99.83 (M)	CBAM attention module + Residual connections	Improved focusing on important features in deep networks.
Alshehri et al. [61]	SA-DCNN	IoTID20 Edge-IIoTset	99.8% (B) 99.76% (B)	Self-Attention + Dynamic weighting	Effective handling of data imbalance in industrial environments (IIoT).

5.3 Hybrid and Emerging Techniques. The modern development of IDS is characterized by the integration of hybrid paradigms that combine the complementary strengths of different algorithms. Emerging methods prioritize not only detection accuracy but also data privacy, decision transparency, and adaptability in decentralized environments.

5.3.1 Federated Learning and Privacy-Preserving IDS. Federated Learning (FL) has emerged as a pivotal technology for orchestrating collaborative model training without the necessity of exchanging source data, which is critical for privacy protection. A practical implementation of this approach on resource-constrained devices was demonstrated by Bhavsar et al. [72], who deployed an FL-IDS system directly on edge devices, specifically on Raspberry Pi, for the protection of automotive IoT. The combination of Logistic Regression (LR) and Convolutional Neural Networks (CNN) enabled them to achieve an accuracy of 94 - 99% on the NSL-KDD and Car-Hacking datasets.

Further exploring deep learning within a federated environment, Nivaashini et al. [73] introduced the FEDDBN-IDS system, which utilizes pre-trained Deep Belief Networks (DBN) and cascaded Restricted Boltzmann Machines (RBM), achieving high efficiency (88 - 98%) on Wi-Fi network data.

Beyond distributed learning, the protection of the model itself is critical. Markovic et al. [74] integrated Differential Privacy methods into a federated Random Forest algorithm, enabling the protection of the system

against inference attacks - attempts to reconstruct training data through the analysis of model responses.

To reduce data transmission latencies and offload central servers, researchers are increasingly turning to Fog and hierarchical architectures. In such systems, data processing occurs at intermediate nodes, such as routers or gateways, located closer to the source of events.

Rehman et al. [75] integrated federated learning directly into the Fog layer of the Industrial IoT. By processing data on intermediate nodes (FFL-IDS), the system was able to react instantly to jamming and spoofing attacks with an accuracy of ~94 - 96%, minimizing latency, which is critical for IIoT.

In complex hierarchical systems, the issue of highly heterogeneous (Non-IID) data across different levels frequently arises. Peng et al. [76] addressed this via Knowledge Distillation. This enabled the effective transfer of "generalized knowledge" from heavyweight upper-level models to lightweight lower-level models, ensuring training stability in a distributed environment.

To protect vehicular networks (CAN), where bandwidth is constrained, Althunayyan et al. [77] employed hierarchical aggregation. Instead of transmitting all updates to a central server, the system first aggregates ANN models and LSTM autoencoders within local vehicle clusters. This facilitate multi-stage threat detection without congesting communication channels.

Comprehensive solutions are emerging at the intersection of Federated Learning and novel security concepts. Bukhari et al. [78] combined spatial (SCNN) and temporal (BiLSTM) models in a federated environment for Wireless Sensor Networks (WSN). Simultaneously, Javeed et al. [79] integrated Federated Learning with the Zero Trust paradigm. Their CNN-BiLSTM-based model achieved impressive accuracy (99.12 - 99.81%) on modern Edge-IIoTset and CIC-IDS-2017 datasets, demonstrating the potential of combining rigorous access verification with decentralized attack detection.

5.3.2 Integration of Explainable AI (XAI). In mission-critical systems, the "black box" nature of neural networks engenders distrust, making the integration of Explainable AI (XAI) methods a necessity. This enables security operators to understand why the system flagged specific activity as an attack.

Kazi F. et al. [34] successfully integrated the SHAP (Shapley Additive Explanations) method into a federated neural network for IoT. This enabled them to achieve an accuracy of 88.2% on the CICIoT2023 dataset and to visualize the contribution of each traffic feature to the decision-making process. In turn, Ullah F. et al. [80] integrated an XAI module into a Transformer-based model, ensuring the interpretability of transfer learning results.

5.3.3 Advanced Hybrid Architectures and Behavior Modeling. Modern approaches extend beyond simple ensembles, integrating heterogeneous methods to enhance detection capabilities and data quality.

An effective strategy involves the fusion of rule-based systems with Deep Learning. Feng L. et al. [27] developed a multi-layer system for the SOME/IP protocol, which combines rigid header verification rules with a Multi-GRU model for payload analysis, achieving nearly 100% accuracy. A similar approach was applied by Sajad E. et al. [26], who integrated the Suricata system with a module based on Fuzzy Logic, enabling a balance between accuracy (96.11%) and processing speed.

The shift from detecting individual packets to analyzing holistic scenarios was demonstrated by Didik S. et al. [40]. In their work on the CREMEv2 dataset, they utilized 1D-CNN to detect sequential attack stages in alignment with the MITRE ATT&CK matrix. The use of auto-dynamic features enabled an F1-score of 0.85 on new, unseen data, outperforming models oriented toward isolated events.

***Table 4* – Performance metrics for selected hybrid and emerging techniques**

Study	Model / Approach	Dataset	Accuracy (%) (Binary / Multi)	Technology / Feature	Key Contribution / Result
Bhavsar et al. [72]	Federated LR + CNN	NSL-KDD Car-Hacking	94 - 99% (B)	Edge Deployment (Raspberry Pi)	Effective protection of automotive IoT without data transmission to the cloud.
Rehman et al. [75]	Fog-enabled Federated CNN	Edge-IIoTset CIC-IDS2017	93.40% (M) 95.80% (M)	Integration into the Fog Layer	Minimization of latency to counter jamming attacks in real-time.
Javeed et al. [79]	Zero-Trust + CNN-BiLSTM (FL)	Edge-IIoTset CIC-IDS-2017	>99.12% (B)	Zero-Trust paradigm in a federated environment	Combining rigorous access verification with decentralized detection.
Bukhari et al. [78]	SCNN-BiLSTM (FL)	WSN-DS	99.7% (M)	Spatial-Temporal models	Adaptation of deep learning for Wireless Sensor Networks (WSN).
Kazi F. et al. [34]	Federated ANN + SHAP	CICIoT2023	88.20% (B/M)	Explainable AI (XAI) - SHAP method	Visualization of decision-making reasons in a federated network.
Feng L. et al. [27]	Hybrid Rules + Multi-GRU	SOME/IP (Auto)	~100.00% (M)	Hybrid: Rules + Deep Learning	Multi-level protection: rapid header filtering + deep payload analysis.
Didik S. et al. [40]	1D-CNN Lifecycle	CREMEv2	0.85 (B) (F1)	Auto-dynamic features	Detection of the full attack lifecycle rather than individual packets.
Gul et al. [81]	WGAN + RF, CNN, MLP	CICIDS2017	98.90% (M)	Generative Adversarial Networks (WGAN)	Data augmentation to solve the critical class imbalance problem.
Sajad E. et al. [26]	Suricata + Fuzzy Logic	Lab Testbed	96.11% (M)	Fuzzy Logic	Balance between detection accuracy and traffic processing speed.

To address the problem of attack data scarcity, researchers are employing generative models. Gul S. et al. [81] applied WGAN (Wasserstein GAN) for data augmentation and a Random Forest classifier for feature selection, which increased the accuracy of a CNN model on the CICIDS2017 dataset to 98%.

To improve the quality of the features themselves, Wenfeng X. and Yongxian F. [57] proposed the use of autoencoders (the LogAE model) in conjunction with XGBoost.

These hybrid solutions represent the forefront of IDS evolution, balancing high performance, generalization capability, and efficiency in the face of decentralized threats.

6. Performance Evaluation and Efficiency Criteria of IDS

Accurate comparison of Intrusion Detection Systems (IDS) necessitates extending beyond basic accuracy metrics. In real-world operational environments, where network traffic is high-speed, anomalies are rare, and attacks are adversarial, the evaluation methodology becomes a critical success factor.

This section analyzes modern performance metrics, operational constraints, and reliability criteria.

6.1 Metric Selection Challenges in Imbalanced Environments. The traditional metric of Accuracy is frequently misleading within the cybersecurity context due to the "accuracy paradox." In real-world networks, the proportion of malicious traffic may constitute less than 1%.

Under such conditions, a trivial model that classifies all traffic as "normal" would achieve 99% accuracy while possessing zero detection efficiency.

For an objective evaluation on imbalanced datasets, it is essential to utilize specialized metrics:

- F1-score: The harmonic mean of Precision and Recall. While this is the de facto standard, it does not account for True Negatives (TN).
- Matthews Correlation Coefficient (MCC): A more robust metric for binary classification. MCC considers all four quadrants of the confusion matrix (TP, TN, FP, FN) and yields a high score only if the classifier performs well on both the positive and negative classes.
- AUC-PR (Area Under the Precision-Recall Curve): Unlike the ROC curve, which can be overly optimistic in the presence of class imbalance, AUC-PR focuses exclusively on the detection efficiency of the minority class (attacks).

6.2 Operational Efficiency and Resource Constraints. High detection accuracy becomes meaningless if the system fails to process traffic in real-time.

For resource-constrained environments (IoT, IIoT, automotive onboard networks), operational metrics become critical:

- Classification Latency (Inference Latency): Defines the time required for the model to process a single packet or flow. For vehicular networks (CAN/SOME/IP), this metric must be less than 1 - 5 ms to ensure movement safety.
- Throughput: The number of packets per second (PPS) the system can process without data loss. This is a key indicator for high-speed backbone networks.
- Energy Efficiency (Energy Consumption): The energy expenditure required to process a unit of information. A critical parameter for battery-powered IoT sensors.
- Memory Requirements (Memory Footprint): The volume of RAM needed to load the model. Transformers, despite their high accuracy, often require gigabytes of memory, rendering them unsuitable for microcontrollers without the application of compression methods (quantization, pruning).

6.3 Reliability and Explainability Metrics. Requirements for modern IDS extend beyond simple classification accuracy to encompass critical aspects of reliability and transparency.

System robustness against targeted manipulations is quantitatively evaluated via the Attack Success Rate (ASR) - the percentage of adversarial examples that successfully bypass defense mechanisms. Consequently, minimizing ASR serves as a key indicator of model reliability.

In parallel, to validate Explainable AI (XAI) methods, metrics of Fidelity and Stability are employed. The former measures the degree of correspondence between the generated explanation and the model's actual internal decision logic, while the latter characterizes the consistency of interpretation under minor input perturbations, ensuring that similar input vectors yield coherent explanations.

6.4 Analysis of Performance Trade-offs and Architectural Constraints. An analysis of experimental data from 2020 - 2025 indicates that no single modern approach is capable of simultaneously maximizing all performance criteria. It is impossible to simultaneously achieve maximum accuracy, minimum latency, and full robustness against adversarial attacks.

Table 5 summarizes the testing results of key algorithm classes according to the metrics defined in sections 6.1-6.3. This synthesis allows researchers to select the optimal method depending on the priority metric.

For critical real-time systems, the priority metric is Inference Latency; therefore, preference is given to optimized ML models, even at the cost of a slight reduction in F1-score.

For threat analytics (SOC), where analysis can occur offline, the key metrics are F1 and MCC, justifying the utilization of resource-intensive Transformers.

For open environments, the critical metric becomes ASR (Attack Success Rate), as high accuracy on test data does not guarantee protection against malicious manipulations.

Thus, modern IDS development is shifting from chasing fractions of a percent in accuracy on legacy datasets to seeking a balance between detection efficiency, processing speed, and reliability. The most promising direction appears to be hybrid architectures that employ lightweight models (ML) for initial filtering and heavyweight models (Transformers) for the deep analysis of suspicious anomalies.

Table 5 – **Performance Trade-off Matrix for Various IDS Classes**

Algorithm Family	Detection Performance	Computational Efficiency	Robustness (Adversarial)	Interpretability (XAI)
Classical ML (DT, RF, XGBoost)	High on known attacks. Degrades on high-dimensional/imbalanced data.	Excellent (Low Latency). Suitable for resource-constrained Edge/IoT devices.	Low. High ASR with minimal perturbations. Prone to evasion attacks.	High. White-box models (e.g., decision paths in DT). Inherently explainable.
Deep Learning (CNN, LSTM, GRU)	Very High. Captures complex non-linear patterns. SOTA on many datasets.	Moderate. Requires GPU acceleration for real-time inference. High energy consumption.	Moderate. Susceptible to gradient-based attacks (FGSM, PGD). Requires adversarial training.	Low. Black-box nature. Requires Post-hoc methods (SHAP, LIME, Grad-CAM).
Transformers (ViT, BERT, Swin)	Superior (SOTA). Best context generalization via Self-Attention mechanisms.	Low. High computational/ memory cost (O(n^2) complexity). High latency without optimization.	High. Attention mechanisms provide better noise robustness, though vulnerable to token attacks.	Moderate. Attention maps offer visual explanations, but internal logic remains complex.
Graph Neural Networks (GNN) (GCN, GAT)	High. Excellent for topological analysis and lateral movement detection.	Low/Moderate. Computationally expensive graph construction and aggregation.	Moderate. Robust to node feature noise, but vulnerable to structural attacks.	Moderate. Edge/Node importance can be visualized to explain attack paths.

7. Applications and Industry Deployments

The practical deployment of Intrusion Detection Systems (IDS) has extended beyond traditional enterprise networks, adapting to the unique security requirements of emerging technologies and critical infrastructures. Current research demonstrates a clear trend toward creating specialized solutions that address the stringent constraints of specific domains: the scarcity of computational resources, the necessity of real-time data processing, requirements for ultra-low latency, and the specifics of industrial protocols.

7.1 General Networks and Cloud Environments. In modern cloud and Software-Defined Networks (SDN), primary research efforts are directed toward enhancing the detection accuracy of complex anomalies and optimizing the processing of high-volume traffic. Transformer-based architectures demonstrate significant potential in this domain; thanks to attention mechanisms, they effectively capture complex relationships between features, achieving accuracies exceeding 93% and reducing false positive rates compared to Recurrent Neural Networks [63]. For performance optimization in SDN, the utilization of accelerated packet processing technologies (DPDK) combined with statistical methods has proven effective, minimizing CPU load even during DDoS attacks [82].

A distinct research vector involves the protection of containerized environments and addressing data quality issues. For Kubernetes clusters, distributed systems are being developed that analyze system calls and offload computation from the host, ensuring an accuracy of over 99% [28]. Simultaneously, Generative Adversarial Networks (GAN) and approaches accounting for the attack lifecycle are successfully applied to overcome class imbalance and improve model generalization across diverse traffic patterns [81, 40].

7.2 Internet of Things (IoT) and Industrial Internet of Things (IIoT). The distinct characteristics of IoT and IIoT, defined by a distributed topology and resource constraints, stimulate the development of "lightweight" solutions with high accuracy. To address these challenges, optimized Deep Learning models are widely applied, specifically LSTMs with data balancing, Self-Attention mechanisms for feature filtering, and Ensemble methods (XGBoost) with oversampling. These approaches demonstrate high efficiency in both general and industrial networks [59, 61, 69, 46, 52, 53].

Federated and Fog-enabled systems are emerging as a key architectural trend for ensuring privacy and scalability in IoT. These systems enable data processing closer to the source, counter jamming and spoofing attacks, and effectively handle heterogeneous data through Knowledge Distillation. Also noteworthy is the successful adaptation of Transformers for the protection of specific protocols, such as MQTT [75, 76,64].

7.3 Vehicular Networks. Security of onboard systems (CAN, Automotive Ethernet) demands a combination of ultra-low latency and impeccable accuracy. In this domain, hybrid approaches combining rigid header verification rules with deep payload analysis (e.g., Multi-GRU for the SOME/IP protocol), as well as adapted Transformers for CAN traffic analysis, have proven effective [27, 65]. The foundation for developing and testing such systems is provided by state-of-the-art datasets derived from real-world network environment traffic [16, 31].

To protect privacy in connected cars and Electronic Control Units (ECU), Federated Learning and hierarchical model aggregation methods are increasingly being implemented. These allow for the detection of injection attacks even on resource-constrained devices [72, 77].

7.4 Critical Infrastructure (SCADA, Power Grids). The protection of Industrial Control Systems (ICS) and power grids focuses on specific protocols and countering targeted manipulations. Research encompasses the development of specialized IDS for the IEC 60870-5-104 protocol, the analysis of data flows within ICS systems, and ensuring the security of Microgrids. A crucial aspect involves addressing data imbalance in critical traffic, where oversampling methods allow for a significant enhancement in detection quality [36, 82, 83].

7.5 Specialized Domains (IoMT, WSN). In highly specialized domains, the architecture of IDS is dictated by unique environmental constraints. For instance, for the Internet of Medical Things (IoMT), hybrid models

(BiLSTM-DNN) adapted to medical traffic are being developed. For Wireless Sensor Networks (WSN), the priority is energy efficiency, achieved through optimized federated algorithms. Furthermore, comprehensive models integrating Zero-Trust principles for the universal protection of heterogeneous devices are gaining widespread adoption [68, 78,79].

8. Challenges, Limitations, and Open Issues

Despite significant progress in algorithm development, Intrusion Detection Systems (IDS) continue to face fundamental obstacles that limit their effectiveness and hinder widespread adoption in real-world scenarios. An analysis of contemporary literature highlights a spectrum of issues encompassing technical, operational, ethical, and research aspects.

8.1 Technical Challenges. One of the most acute problems remains the high rate of False Positives in anomaly-based systems, leading to "alert fatigue" and diminished trust among security operators. The situation is exacerbated by imbalance in training datasets, where normal traffic significantly outweighs attack samples, distorting model performance and rendering the effective detection of rare threats impossible. This vulnerability is actively exploited by malicious actors through Zero-Day and Adversarial attacks, as models trained on historical data often fail to generalize knowledge to new threat vectors.

An additional barrier is the widespread use of encryption, which conceals packet payloads, forcing systems to rely exclusively on metadata or behavioral patterns. Furthermore, the dynamic nature of modern networks, manifested through topology changes or concept drift, complicates the detection of "low-and-slow" attacks. As noted by Genuario et al. [14] and Ziadoon K. et al. [13], although accuracy on benchmark tests approaches perfection, real-world performance and robustness against adversarial examples remain insufficient, particularly in resource-constrained IoT environments.

8.2 Operational and Deployment Challenges. Scaling IDS within large distributed systems encounters the issue of high communication and synchronization overheads, a factor particularly critical for Federated Learning frameworks [11, 20]. The efficiency of global models is further compromised by data heterogeneity (Non-IID) across clients, necessitating the development of complex aggregation mechanisms.

Real-world deployment exposes gaps in integration with existing Security Operations Centers (SOC) and in ensuring observability, particularly within containerized environments, as indicated by Rocha et al. [28]. A fundamental problem remains the low quality and obsolescence of available datasets, which precludes the accurate validation of solutions prior to implementation, as emphasized in numerous reviews [15, 16].

8.3 Ethical Aspects and Privacy Preservation. Deep network traffic analysis inevitably creates a conflict between security and privacy, particularly in decentralized systems containing sensitive data. Although Federated Learning mitigates centralization risks, it introduces new attack vectors, such as user data reconstruction or data poisoning. Ethical IDS deployment necessitates striking a balance between effective monitoring and the prevention of mass surveillance, as well as ensuring algorithmic fairness across diverse user groups.

8.4 Gaps in Current Research. The literature analysis revealed several critical gaps requiring the attention of the scientific community. First, there is a lack of unified comparative evaluation methodologies that incorporate dynamic scenarios, adversarial attacks, and models of the full threat lifecycle. The necessity for updating datasets and developing hybrid approaches is highlighted by Didik S. et al. [40] and Satılmış et al. [21]. Second, the majority of evaluations are confined to controlled experiments, leaving long-term tests in real-world conditions unaddressed. Third, the field of Explainable AI (XAI) remains insufficiently developed for complex models, limiting their interpretability by operators.

A distinct open question is the integration of IDS with emerging technologies, such as Post-Quantum Cryptography, and the creation of standardized benchmarks for Reinforcement Learning (RL). Bridging the gap between high laboratory efficiency and robust, ethical real-world deployment remains the most paramount task for the coming years.

9. Future Directions and Recommendations

The rapid evolution of Intrusion Detection Systems (IDS), driven by advancements in Artificial Intelligence and the exponential growth of vulnerable digital ecosystems, unveils new horizons for research. Based on the analysis of the limitations of contemporary solutions, this section outlines development prospects and provides practical recommendations for creating the next generation of resilient IDS.

9.1 Integration with Emerging Technologies

The future of IDS lies in synergy with advanced technologies, which will allow for overcoming the boundaries of traditional monitoring. A critical step is the integration of Explainable AI (XAI) methods, such as SHAP and LIME, into complex deep learning models. This will enhance decision transparency and operator trust, as already demonstrated by initial integration efforts within federated frameworks [34,80].

To strengthen the security of the algorithms themselves, the utilization of Blockchain in Federated Learning appears promising, protecting model updates from data poisoning attacks. Simultaneously, the development of quantum computing dictates the necessity of transitioning to quantum-resistant encryption and detection algorithms. Infrastructural changes associated with the implementation of 6G networks and Software-Defined Networks (SDN) will require adaptive systems with ultra-low latency. In this context, Hybrid Transformers combined with Fog Computing are set to become the standard for optimizing real-time operations. Furthermore, dynamic response strategies can be implemented via Reinforcement Learning (RL), particularly in its multi-agent variants, allowing the system to autonomously adapt to the adversary's actions [19].

9.2 Research Priorities. The scientific community must concentrate on resolving fundamental problems that hinder the field's development. A primary task is the development of unified dynamic datasets that contain

examples of adversarial attacks in real-time and scenarios reflecting the full attack lifecycle in accordance with the MITRE ATT&CK matrix [40, 15]. Protection against threats in encrypted traffic remains a critical gap. Promising directions here include improving metadata analysis and utilizing Homomorphic Encryption to inspect payloads without decrypting them.

To address unknown threats, it is necessary to advance Transfer Learning and Domain Adaptation methods, which will improve the models' generalization capabilities [84–86]. Targeted research is also required in the sphere of multimodal data fusion, combining network flows with system logs, as well as the development of standardized benchmarks to evaluate robustness against adversarial attacks in federated architectures [87–89]. Another important vector is Active Learning, which will enable the creation of personalized models in environments with heterogeneous data distributions (Non-IID) [84].

Conclusions

In recent years, Intrusion Detection Systems (IDS) have undergone a profound transformation, driven by the integration of advanced Machine Learning, Deep Neural Networks, and privacy-preserving paradigms. This systematic review, covering research from 2020 to 2025, has highlighted the key development vectors of the field. This evolutionary leap has enabled a transition from static signature-based analysis to the dynamic countering of increasingly sophisticated cyber threats.

Research indicates that the process of threat identification and neutralization in modern intelligent IDS relies on the synergy of several technological layers: anomaly detection, localization and preventive measures, and threat interpretation.

Ensemble architectures and Transformer-based models dominate the landscape of anomaly detection methods, providing unprecedented pattern recognition accuracy. These models are capable of detecting zero-day attacks - threats not yet described in databases - by identifying behavioral anomalies in traffic.

The Transformer architecture is capable of autonomously forming a feature hierarchy and allows for the simultaneous processing of the entire input data sequence. This eliminates the bottleneck of sequential computation and ensures significant acceleration of the training process on large datasets. However, a fundamental limitation of the standard Transformer architecture is the quadratic dependence of computational costs on the input sequence length, alongside the need for representative datasets. Furthermore, model implementation requires a careful balance between analysis depth and computational power. The use of ensembles holds the most promise in critical infrastructures for immediate blocking, where the cost of a missed attack or the erroneous interruption of business processes is extremely high. Ensemble models, particularly those based on Boosting (e.g., XGBoost, CatBoost) or specialized techniques (Balanced Random Forest), allow the model to better focus on "rare events" (attacks) without sacrificing overall accuracy. Furthermore, ensembles utilizing diverse mathematical decision-making algorithms are significantly harder to compromise. However, ensemble models are susceptible to overfitting.

There is a rapid rise in the popularity of Federated and Fog-enabled frameworks, which enable local threat detection while adhering to strict privacy requirements. Instead of transmitting gigabytes of traffic to a distant cloud for analysis, Fog nodes (routers, gateways) process data locally, reducing attack response time by orders of magnitude. This allows not merely for intrusion detection but for instant blocking before substantial damage occurs. Additionally, Fog nodes act as filters; they analyze traffic on-site and transmit only "suspicious" patterns or aggregated reports to the cloud, thereby reducing network load.

The emergence of Explainable AI (XAI) approaches and models that account for the attack lifecycle enhances the systems' capacity for generalization and decision interpretation. Such approaches reduce False Positives by, for example, flagging specific features like packet size or a specific flag in a TCP header. This empowers the analyst to make the final informed decision.

A crucial component of these models is the dataset. This study proposes a multidimensional taxonomy and a critical analysis of contemporary datasets. This analysis revealed significant progress toward generating datasets based on real-world network traffic, yet simultaneously highlighted persistent challenges regarding unification and the dynamic representation of threats. Although performance evaluations consistently demonstrate accuracy exceeding 98% on benchmarks, the real-world application of many solutions remains limited. The primary obstacles include class imbalance, vulnerability to adversarial attacks, scaling difficulties in environments with heterogeneous data (Non-IID), and the opacity of complex models.

Requirements for modern Intrusion Detection Systems (IDS) are shifting from basic classification accuracy toward complex parameters of resilience and computational process transparency (Attack Success Rate (ASR), Fidelity, and Stability metrics). Synthesizing this knowledge, this review bridges a critical gap in the literature by offering a holistic and forward-looking vision of the field's development, in contrast to previous works that were often restricted to a narrow focus.

The synergy of technological layers and the transition toward hybrid and decentralized architectures evidence the qualitative evolution of IDS technologies. Future progress depends on bridging the divide between high accuracy indicators in experimental conditions and operational stability in real-world deployment. It is the development of unified testing standards, the enhancement of robustness against adversarial attacks, and the integration of explainability mechanisms that will serve as the foundation for creating the next generation of adaptive and reliable security systems.

Conflicts of interest

The authors declare that they have no conflicts of interest in relation to the current study, including financial, personal, authorship, or any other, that could affect the study, as well as the results reported in this paper.

Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technologies when creating the current work.

References

1. Anderson, J. (2012), “Computer security threat monitoring and surveillance”, *International Journal of Intelligence Science*, vol. 2, Nno. 4A, available at: https://www.scirp.org/reference/referencespapers?referenceid=613257
2. Denning, D. (1987), “An Intrusion-Detection Model”, *IEEE Transactions on Software Engineering*, vol. 13(2), pp. 222–232, doi: https://doi.org/10.1109/TSE.1987.232894
3. Gavrylenko, S. and Hornostal, O. (2023), “Application of heterogeneous ensembles in problems of computer system state identification”, *Advanced Information System*, vol. 7, no. 4, pp. 5–12, doi: https://doi.org/10.20998/2522-9052.2023.4.01
4. Gavrylenko, S., Chelak, V. and Hornostal, O. (2022), “Construction Method Of Fuzzy Decision Trees For Identification The Computer System State”, *Proceedings of the 32th International Scientific Symposium Metrology and Metrology Assurance* (MMA), Sozopol, Bulgaria, pp. 1–5, doi: https://doi.org/10.1109/MMA55579.2022.9992878
5. Gavrylenko, S., Poltoratskyi, V. and Nechyporenko, A. (2024), “Intrusion detection model based on improved transformer”, *Advanced Information Systems*, vol. 8, no. 1, pp. 94–99, doi: https://doi.org/10.20998/2522-9052.2024.1.12
6. Ashraf, J., Nour, M, Khurshid, H., E., Debie, Waqas H. and Wahab, A. (2020), “A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions”, *Electronics*, vol. 9, article number 1197, doi: https://doi.org/10.3390/electronics9071177
7. Khraisat, A. and Alazab, A. (2021), “A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges”, *Cybersecurity*, vol. 4, article number 18, doi: https://doi.org/10.1186/s42400-021-00077-7
8. Seyfollahi, A. and Ghaffari, A. (2021), “A Review of Intrusion Detection Systems in RPL Routing Protocol Based on Machine Learning for IoT Applications”, *Wireless Commu. and Mobile Computing*, vol. 32, doi: https://doi.org/10.1155/2021/8414503
9. Stavroula, B., Saer, E., Velivasaki, A. Terpsichori-Helen. Voulkidis, A. and Zahariadis, T., (2021), “A Review of Tabular Data Synthesis Using GANs on an IDS Dataset”, *Information*, vol. 12, doi: https://doi.org/10.3390/info12090375
10. Rabbani, M., Wang, Y., Khoshkangini, R., Jelodar, H., Zhao, R., Bagheri Baba Ahmadi, S. and Ayobi, S. (2021), “A Review on Machine Learning Approaches for Network Malicious Behavior Detection in Emerging Technologies”, *Entropy*, vol. 23(5), article number 529, doi: https://doi.org/10.3390/e23050529
11. Agrawal, S., Sarkar, S., Aouedi, O., Yenduri, G., Piamrat, K., Bhattacharya, S., Reddy, P. and Gadekallu, T. (2021), “Federated Learning for Intrusion Detection System: Concepts, Challenges and Future Directions”, *Computer communication*, vol. 195, no. C, pp. 346 –361, doi: https://doi.org/10.48550/arXiv.2106.09527 .
12. Chelak, V., Hornostal, O., Chelak, Y. and Gavrylenko, S. (2025), “Advanced methods for classification quality assessment leveraging roc analysis and multidimensional confusion matrix”, *Advanced Information Systems*, vol. 9, no. 1, pp. 24–34, doi: https://doi.org/10.20998/2522-9052.2025.1.03
13. Ziadoon K., Robiah, Y., Al-Bander, B., Saif, A. and Qusay, K. (2023), “Meta-Analysis and Systematic Review for Anomaly Network Intrusion Detection Systems: Detection Methods, Dataset, Validation Methodology, and Challenges”, *IET Networks*, vol. 13, issue 5-6, pp. 339–376, doi: https://doi.org/10.48550/arXiv.2308.02805
14. Genuario, F., Santoro, G., Giliberti, M., Bello, S., Zazzera, E. and Impedovo, D. (2024), “Machine learning-based methodologies for cyber-attacks and network traffic monitoring”, *Electrical Engineering*, vol. 5(11), article number 74,1 doi: https://doi.org/10.20944/preprints202407.0029.v1
15. Akbar, K., Yasir, M., Hakim A. and Bashir, M. (2024), “From Bytes to Insights: A Systematic Literature Review on Unraveling IDS Datasets for Enhanced Cybersecurity Understanding”, *IEEE Access*, doi: https://doi.org/10.1109/ACCESS.2024.3392338
16. Miki, V., Bridges, R, Iannacone, R., Hollifield, M., Moriano, S., Hespeler, P., Bill, K. and Frank, C. (2024), “A comprehensive guide to CAN IDS data and introduction of the ROAD dataset”, *PLOS ONE*, vol. 19., e0296879, doi: https://doi.org/10.1371/journal.pone.0296879
17. Fteiha, B., Zia, H., Zeyadeh, M., Hazeem, R., Obaidat, H. and Ghannam, R. (2025), “Enhancing IoT network security: a literature review of intrusion detection systems and their adaptability to emerging threats”, *Open Computer Science*, vol. 15, doi: https://doi.org/10.1515/comp-2025-0046
18. Gavrylenko, S., Hornostal, O. and Chelak, V. (2022), “Research of Methods of Identifying the Computer Systems State based on Bagging Classifiers”, *2022 IEEE 3rd KhPI Week on Advanced Technology* (KhPIWeek), pp. 1–6, doi: https://doi.org/10.1109/KhPIWeek57572.2022.9916439
19. Finistrella, S., Mariani, S. and Zambonelli, F. (2025), “Multi-Agent Reinforcement Learning for Cybersecurity: Classification and survey”, *Intelligent Systems with Applications*, vol. 26, doi: https://doi.org/10.1016/j.iswa.2025.200495
20. Latif, N., Ma, W. and Hafizm, A. (2025), “Advancements in securing federated learning with IDS: a comprehensive review of neural networks and feature engineering techniques for malicious client detection”, *Artificial Intelligence Review*, vol. 58, article number 91, doi: https://doi.org/10.1007/s10462-024-11082-w
21. Satilmiş, H., Akleylek, S. and Tok, Z. Y. (2024), “A Systematic Literature Review on Host-Based Intrusion Detection Systems”, *in IEEE Access*, vol. 12, pp. 27237–27266, doi: https://doi.org/10.1109/ACCESS.2024.3367004
22. Poltoratskyi, V. and Gavrylenko, S. (2025), “Improved Feature Tokenizer Transformer”, *2025 IEEE 6th KhPI Week on Advanced Technology (KhPIWeek)*, Kharkiv, Ukraine, pp. 1–7, doi: https://doi.org/10.1109/KhPIWeek61436.2025.11288603
23. Semenov, S., Gavrylenko, S. and Chelak, V. (2016), “Developing parametrical criterion for registering abnormal behavior in computer and telecommunication systems on the basis of economic tests”, *Actual Problems of Economics*, vol. 4, pp. 451–459, doi: https://doi.org/10.15587/1729-4061.2021.233417
24. Gavrylenko, S., Chelak, V. and Hornostal, O. (2020), “Research of Intelligent Data Analysis Methods for Identification of Computer System State”, *Proceedings of the 30th International Scientific Symposium Metrology and Metrology Assurance (MMA)*, Sozopol, Bulgaria, pp. 1–5. doi: https://doi.org/10.1109/MMA49863.2020.9254252
25. Gavrylenko, S., Chelak, V. and Semenov, S. (2022), “Development of Method for Identification the Computer System State based on the Decision Tree with Multi-Dimensional Nodes”, *Radio Electronics, Computer Science, Control (RECSC)*, vol. 2, pp.113–121, doi: https://doi.org/10.15588/1607-3274-2022-2-11
26. Sajad, E., Cemil, O. and Navaei, D. (2021), “The Anomaly- and Signature-Based IDS for Network Security Using Hybrid Inference Systems”, *Mathematical Problems* in *Engineering*, pp.1–10, doi: https://doi.org/10.1155/2021/6639714

27. Feng, L., Zhenyu, Y., Zhaojing, Z Wang, Z., Bowen, W. and Mingzhi, W. (2023), "A Multi-Layer Intrusion Detection System for SOME/IP-Based In-Vehicle Network", *Sensors*, vol. 23, doi: https://doi.org/10.3390/s23094376
28. Rocha, S., Mendonça, F., Puttini, R., Nunes, Rafael and Amvame-Nze, G. (2023), "DCIDS - Distributed Container IDS", *Applied Sciences*, vol. 13, article number 9301, doi: https://doi.org/10.3390/app13169301
29. Semenov, S., Krupska-Klimczak, M., Czapla, R., Krzaczek, B., Gavrylenko, S., Poltorazkiy, V. and Zozulia, V. (2025), "Intrusion Detection Method Based on Preprocessing of Highly Correlated and Imbalanced Data", *Applied Sciences*, vol. 15 (8), article number 4243, doi: https://doi.org/doi: https://doi.org/10.3390/app15084243
30. Gavrylenko, S., Zozulia, V. and Khatsko N. (2023), "Methods for Improving the Quality of Classification on Imbalanced Data", *Proc. of the IEEE 4th KhPI Week on Advanced Technology*, pp. 1–5, doi: https://doi.org/10.1109/KhPIWeek61412.2023.10312879
31. Brooke, L. and Weizhi, M. (2024), "Can-train-and-test: A Curated CAN Dataset for Automotive Intrusion Detection", *Computers and Security*, vol. 140, doi: https://doi.org/10.1016/j.cose.2024.103777
32. Ferrag, M., Friha, O., Hamouda, D., Maglaras, L. and Janicke, H. (2022), "Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning", *IEEE Access*, vol. 10, pp. 40281–40306, doi: https://doi.org/10.1109/ACCESS.2022.3165809
33. Sharmila, B., Nandini, B., Kavitha, S., and Anand S. (2024), "Performance Evaluation of Parametric and Non-Parametric Machine Learning Models using Statistical Analysis for RT-IoT2022 Dataset", *Journal of Scientific and Industrial Research*, vol. 83, pp. 864–872. doi: https://doi.org/10.56042/jsir.v83i8.7437
34. Kazi, F., Samrat, D., Mehrin, A., Risala. K. Rashid, M., Su, C. and Mazumder, R. (2025), "Federated XAI IDS: An Explainable and Safeguarding Privacy Approach to Detect Intrusion Combining Federated Learning and SHAP", *Future Internet*, vol. 17, article number 234. doi: https://doi.org/10.3390/fi17060234
35. Dadkhah, S., Neto, E., Ferreira, R., Molokwu, R., Sadeghi, S. and Ghorbani, A. (2024), "CICIoMT2024: A benchmark dataset for multi-protocol security assessment in IoMT", *Internet of Things*, vol. 28, article number 101351, doi: https://doi.org/10.1016/j.iot.2024.101351
36. Arifin, M. et al. (2024), "A Novel Dataset for Experimentation With Intrusion Detection Systems in SCADA Networks Using IEC 60870-5-104 Standard", *IEEE Access*, vol. 12, pp. 170553–170569, doi: https://doi.org/10.1109/ACCESS.2024.3473895
37. Dehlaghi-Ghadim, A., Moghadam, M. H., Balador, A. and Hansson H. (2023), "Anomaly Detection Dataset for Industrial Control Systems", *IEEE Access*, vol. 11, pp. 107982–107996 doi: https://doi.org/10.1109/ACCESS.2023.3320928.
38. Zhibo, Z., Benjamin, T., Shabnam, K., Hemanshu, P. and Jiankun, H. (2025), "UNSW-MG24: A Heterogeneous Dataset for Cybersecurity Analysis in Realistic Microgrid Systems", *IEEE Open Journal of the Computer Societ*, pp. 1–12, doi: https://doi.org/10.1109/OJCS.2025.3564266
39. Marzia, Z., Dhaval, U. and Chung-Horng, L. (2023), "Validation of a Machine Learning-based IDS Design Framework using ORNL Datasets for Power System with SCADA" *IEEE Access*, doi: https://doi.org/10.1109/ACCESS.2023.3326751
40. Didik, S., Ying-Dar, L., Miel V., Ren-Hung, H., Yuan-Cheng, L., Laurens, D., Tim, W., Bruno, V. and Filip, De T. (2024), "Improving Generalization of ML-Based IDS With Lifecycle-Based Dataset, Auto-Learning Features and Deep Learning", *IEEE Transactions on Machine Learning in Communications and Networking*, vol. 2, pp. 645–662, doi: https://doi.org/10.1109/TMLCN.2024.3402158
41. Li, Q., Wang, B., Wen, X. and Chen, Y. (2025), "Malicious traffic prediction model for ResNet based on Maple-IDS dataset", *PLOS One*, vol. 20, doi: https://doi.org/10.1371/journal.pone.0322000
42. Yusof, M., Hafiz, M., Almohammedi, A. and Shepelev, V. (2022), "Visualizing Realistic Benchmarked IDS Dataset: CIRA-CIC-DoHBrw-2020", *IEEE Access*, vol. 10, pp. 94624–94642, doi: https://doi.org/10.1109/ACCESS.2022.3204690
43. Herzalla, D., Lunardi W. and Andreoni, M. (2023), "TII-SSRC-23 Dataset: Typological Exploration of Diverse Traffic Patterns for Intrusion Detection", *IEEE Access*, vol. 99, doi: https://doi.org/10.1109/ACCESS.2023.3319213
44. Chelak, V., Hornostal, O., Chelak, Y. and Gavrylenko, S. (2025), "Decision Tree Construction Method using Cuckoo Search for Computer System State Identification", *2025 IEEE 6th KhPI Week on Advanced Technology (KhPIWeek)*, pp. 1–6, doi: https://doi.org/10.1109/KhPIWeek61436.2025.11288613
45. Gavrylenko, S., Chelak, V. and Hornostal, O. (2021), "Ensemble Approach Based on Bagging and Boosting for Identification the Computer System State", *2021 XXXI International Scientific Symposium Metrology and Metrology Assurance (MMA), Bulgaria*, 2021, pp. 1–7, doi: https://doi.org/10.1109/MMA52675.2021.9610949
46. Eljialy, U., Mohammed Y. and Ahmad, S. (2024). "Novel Framework for an Intrusion Detection System Using Multiple Feature Selection Methods Based on Deep Learning", *Tsinghua Science and Technology*, vol. 29., pp. 949–959. doi: https://doi.org/10.26599/TST.2023.9010032
47. Gavrylenko, S. and Hornostal, O. (2023), "Study of Methods for Improving the Meta-Algorithm of the Bagging Classifier", *Proceedings of the IEEE 4th KhPI Week on Advanced Technology (KhPIWeek)*, pp. 1–6, doi: https://doi.org/10.1109/KhPIWeek61412.2023.10312977
48. Gavrilenko, S. and Sheverdin, I. (2021), "Exploration of the computer system identification method based on the "Isolation Forest" algorithm", *Radio Electronics, Computer Science, Control*, vol. 1(56), pp. 105–116. doi: https://doi.org/10.15588/1607-3274-2021-1-11
49. Ali, M., Durad, M., Usman, H., Mohsin, A., Muhammad, S., Mujlid, H. and Carsten, H. (2023), "Effective network intrusion detection us stacking-based ensemble approach", *International Journal of Information Security*, vol. 22, pp. 1–18, doi: https://doi.org/10.1007/s10207-023-00718-7
50. Amit, S., Jay, P., Gaurav, K., Praphula, J. and Loknath, A. (2024), "Intrusion Detection System", *Journal of Database Management*, vol. 35, doi: https://doi.org/10.4018/JDM.338276
51. Josy, V. and Balachandra, M. (2021), "An Efficient IDS Framework for DDoS Attacks in SDN Environment", *IEEE Access*, vol. 9, pp. 69680–69699. doi: https://doi.org/10.1109/ACCESS.2021.3078065.
52. Thi-Thu-Huong, L., Yustus, O. and Howon, K. (2022), "XGBoost for Imbalanced Multiclass Classification-Based Industrial Internet of Things Intrusion Detection Systems", *Sustainability*, vol. 14, doi: https://doi.org/10.3390/su14148707
53. Doghramachi, D. and Siddeeq A. (2023), "Internet of Things (IoT) Security Enhancement Using XGboost Machine Learning Techniques", *Computers, Materials and Continua*, vol. 77, pp. 717–732. doi: https://doi.org/10.32604/cmc.2023.041186

54. Sura, E., Baydogmus, K., and Onder, D. (2023), "An ensemble learning based IDS using Voting rule: VEL-IDS. PeerJ", *Computer Science*, vol. 9. article number 1553, doi: https://doi.org/10.7717/peerj-cs.1553
55. Mhamad, B., Rakesh, R. K., Mohammad, H., Zubair, A., Arshad, A., Syed, I. Y., Mohammad, N. A., Nikhat, P. (2024), "Building a Cloud-IDS by Hybrid Bio-Inspired Feature Selection Algorithms Along With Random Forest Model", *IEEE Access*, vol. 12, pp. 8846–8874, doi: https://doi.org/10.1109/ACCESS.2024.3353055
56. Aldabash, O. and Akay, M. (2024), "WS-AWRE: Intrusion Detection Using Optimized Whale Sine Feature Selection and Artificial Neural Network Weighted Random Forest Classifier", *Applied Sciences*, vol. 14, doi: https://doi.org/10.3390/app14052172
57. Wenfeng, X. and Yongxian, F. (2022), "Intrusion Detection Systems Based on Logarithmic Autoencoder and XGBoost", *Security and Communication Networks*, vol. 7, pp. 1–8, doi: https://doi.org/10.1155/2022/9068724
58. Nuaimi, T., Zaabi, S., Alyilieli, M., AlMaskari, M., Alblooshi, S., Alhabsi, F., Yusof, M. F. and Al Badawi, A. (2023), "A Comparative Evaluation of Intrusion Detection Systems on the Edge-IIoT-2022 Dataset", *Intelligent Systems with Applications*, vol. 20, article number 200298,. doi: https://doi.org/10.1016/j.iswa.2023.200298
59. Ridha H., S., Dong W. and Mansour A. (2024), "Enhanced Intrusion Detection with LSTM-Based Model, Feature Selection, and SMOTE for Imbalanced Data", *Applied Sciences*, vol. 14, no. 2, doi: https://doi.org/10.3390/app14020479
60. Belarbi, O., Khan, Aftab, C., P. and Spyridopoulos, T. (2022), "An Intrusion Detection System based on Deep Belief Networks", *Lecture Notes in Computer Science*, doi: https://doi.org/10.48550/arXiv.2207.02117
61. Alshehri, M., Saidani, O., Alrayes, F., Abbasi, S. and Ahmad, J. (2024), "A Self-Attention-Based Deep Convolutional Neural Networks for IIoT Networks Intrusion Detection", *IEEE Access*, vol. 12, pp. 45762–45772, doi: https://doi.org/10.1109/ACCESS.2024.3380816
62. Gavrylenko, S. and Poltoratskyi, V. (2024), "Detection Computer Network Intrusion Using Deep Neural Networks", *2024 IEEE 5th KhPI Week on Advanced Technology (KhPIWeek)*, pp. 1–5, doi: https://ieeexplore.ieee.org/document/10878100
63. Long, Z., Yan, H., Shen, G., Zhang, X., He, H. and Cheng, L. (2024), "A Transformer-based network intrusion detection approach for cloud security", *Journal of Cloud Computing*, vol. 13, doi: https://doi.org/10.1186/s13677-023-00574-9
64. Safi, U., Jawad, A., Muazzam, K., Boulila, M., Koubaa, W., Jan, A., and Ullah, S. (2023). "TNN-IDS: Transformer neural network-based intrusion detection system for MQTT-enabled IoT Networks", *Computer Network*, vol. 237. article number 110072, doi: https://doi.org/10.1016/j.comnet.2023.110072
65. Hyunjun, J. and Deok-Hwan, K. (2024), "Intrusion Detection Using Transformer in Controller Area Network", *IEEE Access*, vol. 12, pp. 121932–121946, doi: https://doi.org/10.1109/ACCESS.2024.3452634.
66. Ghadermazi, J., Hore, S., Shah, A. and Bastian, N. D. (2025), "GTAE-IDS: Graph Transformer-Based Autoencoder Framework for Real-Time Network Intrusion Detection", *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 4026–4041, doi: https://doi.org/10.1109/TIFS.2025.3557741
67. Safi, U., Muazzam, K., Jawad, K., Shaukat, S., Zil, H., Tahir, M., Pitropakis, N., Khan, A. and Buchanan, W. (2022), "HDL-IDS: A Hybrid Deep Learning Architecture for Intrusion Detection in the Internet of Vehicles", *Sensors*, vol. 2, article number 1340, doi: https://doi.org/10.3390/s22041340
68. Benahmed, H., M'hamedi, M., Merzoug, M., Hadjila, M., Bekkouche, A., Etchiali, A. and Said, M. (2025), "HBiLD-IDS: An Efficient Hybrid BiLSTM-DNN Model for Real-Time Intrusion Detection in IoMT Networks", *Information*, vol. 16, article number 669, doi: https://doi.org/10.3390/info16080669
69. Sandeepkumar R., Prathyusha, S., Nuruzzaman, F., Whaiduzzaman, A. and Aziz S. (2024), "Deep-IDS: A Real-time Intrusion Detector for IoT Nodes using Deep Learning", *IEEE Access*, doi: https://doi.org/10.1109/ACCESS.2024.3396461
70. Zaccagnino, R., Guarino, A., Cirillo, A. and Lettieri, N. (2023), "Towards a Geometric Deep Learning-Based Cyber Security: Network System Intrusion Detection Using Graph Neural Networks", *20-th International Conference on Security and Cryptography*, pp. 394–401, doi: https://doi.org/10.5220/0012085700003555
71. Hai, Z., Haojie, Z., Wei, L., Di L. and Yinchun, K. (2025), "HiViT-IDS: An Efficient Network Intrusion Detection Method Based on Vision Transformer", *Sensors*, vol. 25, article number 1752, doi: https://doi.org/10.3390/s25061752
72. Bhavsar, M., Bekele Y., Roy, K. Kelly, C. and Limbrick, D. (2024), "FL-IDS: Federated Learning-Based Intrusion Detection System Using Edge Devices for Transportation IoT", *IEEE Access*, vol. 12, pp. 52215–52226, doi: https://doi.org/10.1109/ACCESS.2024.3386631.
73. Nivaashini, M., Suganya, E., Sountharrajan, S., Prabu, M. and Bavirisetti, D. (2024), "FEDDBN-IDS: Federated Deep Belief Network-based Wireless Network Intrusion Detection System", *EURASIP Journal on Information Security*, vol. 2024, article number 8, doi: https://doi.org/10.1186/s13635-024-00156-5
74. Markovic, T., Leon, M., Buffoni, D., and Punnekkat, S. (2024), "Random forest with differential privacy in federated learning framework for network attack detection and classification", *Applied Intelligence*, vol. 54, pp. 1–-22. doi: https://doi.org/10.1007/s10489-024-05589-6
75. Rehman, T., Tariq, N., Khan, F. A. and Rehman, S. U. (2025), "FFL-IDS: A Fog-Enabled Federated Learning-Based Intrusion Detection System to Counter Jamming and Spoofing Attacks for the Industrial Internet of Things", *Sensors*, vol. 25, article number 10, doi: https://doi.org/10.3390/s250100
76. Peng, H., Wu, C. and Xiao, Y. (2025), "FD-IDS: Federated Learning with Knowledge Distillation for Intrusion Detection in Non-IID IoT Environments", *Sensors*, vol. 25, article number 4309, doi: https://doi.org/10.3390/s25144309
77. Althunayyan, M., Javed, A. and Rana, O. (2024), "A Robust Multi-Stage Intrusion Detection System for In-Vehicle Network Security using Hierarchical Federated Learning", *Vehicular Comm.*, vol. 49, doi: https://doi.org/10.48550/arXiv.2408.08433
78. Bukhari, S., Zafar, M., Abou, M., Moosavi, S., Mansoor, M., Muaaz, M. and Sanfilippo, F. (2024), "Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability", *Ad Hoc Networks*, vol. 155, article number 103407, doi: https://doi.org/10.1016/j.adhoc.2024.103407
79. Javeed, D., Saeed, M., Adil, M., Kumar, P. and Jolfaei, A. (2024), "A federated learning-based zero trust intrusion detection system for Internet of Things", *Ad Hoc Networks*, vol. 162., doi: https://doi.org/10.1016/j.adhoc.2024.103540
80. Ullah, F., Ullah, S., Srivastava, G. and Lin, J. (2024), "IDS-INT: Intrusion detection system using transformer-based transfer learning for imbalanced network traffic", *Dig. Comm. and Networks*, pp. 190–204. doi: https://doi.org/10.1016/j.dcan.2023.03.008

81. Gul, S., Sobia, S., Sanay, M., Adeel A. and Azam, M. (2024), "WGAN-DL-IDS: An Efficient Framework for Intrusion Detection System Using WGAN, Random Forest, and Deep Learning Approaches", *Computers*, vol. 14, article number 5, doi: https://doi.org/10.3390/computers14010004
82. Semenov, S., Mozhaiev, O., Kuchuk, N., Mozhaiev, M., Tiulieniev, S., Gnusov, Yu., Yevstrat, D.,Chyrva, Y., Kuchuk, H. (2022), "Devising a procedure for defining the general criteria of abnormal behavior of a computer system based on the improved criterion of uniformity of input data samples", *Eastern-European Journal of Enterprise Technologies*, vol. 6(4-120), pp. 40–49, doi: https://doi.org/10.15587/1729-4061.2022.269128
83. Kuchuk, H., Kalinin, Y., Dotsenko, N., Chumachenko, I. and Pakhomov, Y. (2024), "Decomposition of integrated high-density IoT data flow", *Advanced Information Systems*, vol. 8, no. 3, pp. 77–84, doi: https://doi.org/10.20998/2522-9052.2024.3.09
84. Kelli, V., Argyriou, V., Lagkas, T., Fragulis, G., Grigoriou, E. and Sarigiannidis, P. (2021), "IDS for Industrial Applications: A Federated Learning Approach with Active Personalization", *Sensors*, vol. 21, doi: https://doi.org/10.3390/s21206743
85. Jia, H., Zhen, C., Sheng-Zheng, L., Hao, Z. and Hai-Xia L. (2024), "Improved Intrusion Detection Based on Hybrid Deep Learning Models and Federated Learning", *Sensors*, vol. 24., article number 4002, doi: https://doi.org/10.3390/s24124002
86. Fatma, A., Zakariah, M., Mohammed, M. D. and Wadii, B. (2023), "Deep Neural Decision Forest (DNDF): A Novel Approach for Enhancing Intrusion Detection Systems in Network Traffic Analysis", vol. 23, doi: https://doi.org/10.3390/s23208362
87. Minxiao V., Ning, Y., Yanhui, G. and Ning, W. (2024), "Learn-IDS: Bridging Gaps between Datasets and Learning-Based Network Intrusion Detection", *Electronics*, vol. 13, pp. 1072, doi: https://doi.org/10.3390/electronics13061072
88. Asaad, B., Habaebi, M., Elsheikh, E., Islam, Md and Eldin, S. (2023), "The Effect of Dataset Imbalance on the Performance of SCADA Intrusion Detection Systems", *Sensors*, vol. 23, article number 758, doi: https://doi.org/10.3390/s23020758
89. Bakro, M., Kumar, R. R., Husain, M., Ashraf, Z., Ali, A. and Yaqoob, S. I. (2024), "Building a Cloud-IDS by Hybrid Bio-Inspired Feature Selection Algorithms Along With Random Forest Model", *IEEE Access*, vol. 12, pp. 8846–8874, doi: https://doi.org/10.1109/ACCESS.2024.3353055

Received (Надійшла) 05.01.2026
Accepted for publication (Прийнята до друку) 25.03.2026

ABOUT THE AUTHORS / ВІДОМОСТІ ПРО АВТОРІВ

Полторацький Вадим Олександрович – магістрант кафедри комп'ютерної інженерії та програмування, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Vadym Poltoratskyi – Master's Student of Computer Engineering and Programming Department, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: Vadim.poltoratsky@gmail.com; ORCID Author ID: https://orcid.org/0009-0003-5312-4939;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=58910498600&origin=resultslist.

Гавриленко Світлана Юріївна – доктор технічних наук, професорка, професорка кафедри "Комп'ютерна інженерія та програмування", Національний технічний університет "Харківський політехнічний інститут", професорка кафедри Харківського національного університету радіоелектроніки, Харків, Україна;
Svitlana Gavrylenko – Doctor of Technical Science, Professor, Professor of the Department of Computer Engineering and Programming, National Technical University «Kharkiv Polytechnic Institute», Professor of the Department at Kharkiv National University of Radio Electronics, Kharkiv, Ukraine;
e-mail: gavrilenko08@gmail.com; ORCID Author ID: https://orcid.org/0000-0002-6919-0055;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57189042150.

Еволюція систем виявлення вторгнень: всебічний огляд сучасних наборів даних, методів глибокого навчання та архітектурних викликів

В. О. Полторацький, С. Ю. Гавриленко

Анотація. Системи виявлення вторгнень (СВВ) залишаються ключовим елементом кібербезпеки. Вони швидко еволюціонують, щоб протистояти дедалі складнішим загрозам у різних середовищах, таких як Інтернет речей (IoT), промисловий Інтернет речей (IIoT), транспортні мережі та критична інфраструктура. Це дослідження представляє систематичний огляд літератури з 2020 по 2025 роки, базується на сучасних дослідженнях і розглядає інтеграцію машинного навчання (ML), глибокого навчання (DL), федеративного навчання (FL) та нових гібридних технік в СВВ, узагальнюючи прогрес їх функціонування. Ключові тренди включають помітний перехід до архітектур глибокого навчання, зокрема, трансформерів та візуальних трансформерів для покращеного розпізнавання патернів. Також спостерігається впровадження федеративного навчання та систем на базі туманних обчислень, що забезпечують приватність і вирішують проблеми децентралізації даних та їхньої неоднорідності (Non-IID). Крім того, зростає увага до пояснюваного ШІ (XAI), наборів даних на основі життєвого циклу атак та стійкості моделей до змагальних атак. Огляд пропонує всебічну класифікацію систем за багатьма критеріями, що. дозволяє повноцінно описати та порівняти різні рішення. У роботі критично оцінюються сучасні набори вхідних даних, а також проводиться порівняльний аналіз ефективності різних методологій виявлення вторгнень. Отримано, що хоча точність роботи алгоритмів на стандартних тестових наборах даних часто перевищує 98%, залишається низка невирішених проблем. Серед них – дисбаланс класів, здатність виявляти нові та невідомі загрози, масштабування в умовах реальної експлуатації та етичні питання конфіденційності. В огляді також обговорюються проблеми та обмеження сучасних методів, вказується на брак уніфікованих датасетів, перевірку ефективності моделей в умовах реальної експлуатації та адаптивного захисту від атак нульового дня й зашифрованого трафіку. Він пропонує дорожню карту для створення більш стійких, децентралізованих та зрозумілих СВВ.

Ключові слова: машинне навчання; системи виявлення вторгнень; класифікація даних; нейронні мережі; глибоке навчання; моделі-трансформери; передобробка даних; ключові показники ефективності..