FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 10 No. 14, June, 2026, pp 157 – 163
DOI: https://doi.org/10.33003/fjs-2026-1014-5147

Comparative Assessment of Networks and Datasets Utilized in IDS/IPS Evaluation

[1]Glory Nosawaru Edegbe, [1]Esosa Enoyoze, [2]Ijegwa David Acheme and *[3]Ali Abubakar Musah

[1]Dept. of Computer Science, Edo State University Iyamho, Edo State, Nigeria.
[2]Department of Computer Science, Wigwe University, Isiokpo, River State, Nigeria.
[3]Department of Computer Science, Auchi Polytechnic, Auchi, Edo State, Nigeria.

*Corresponding authors' email: itmusah@gmail.com

Received: 25 May 2026
Accepted: 02 Jul. 2026
Published: 18 Aug. 2026

ABSTRACT
Most modern networks depend on Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) as core defense system against an increasingly expanding number of cyber threats. This is the reason why research effort over the years has concentrated on improving these systems, while attention is now been directed at the network settings in which they are tested. In this paper, we systematically review the IDS/IPS literature and discuss the evaluation environments and benchmark datasets used to evaluate detection performance, e.g., KDD Cup 99, NSL-KDD, UNSW-NB15, CICIDS2017, and Bot-IoT. The analysis shows that the popular datasets like the KDD Cup 99 are still in widespread use despite their known limitations, such as duplicate records and attack profiles that do not reflect modern threats. Nevertheless, the adoption of other recent datasets such as CICIDS2017 and Bot-IoT that capture more realistic traffic, and include IoT-specific scenarios, is still modest compared to their older counterparts. The review also shows that experiments are mostly based on artificial and not operational traffic and are mostly limited to laboratory and not production settings, thus limiting the external validity of reported results. Taken together, these observations establish a persistent discrepancy between benchmark settings and the realities of operational networks. The paper ends with practical recommendations to assist researchers and practitioners to choose evaluation environments to enhance the realism, dependability and transferability of IDS/IPS solutions.

Keywords: Intrusion Detection System (IDS), Intrusion Prevention System (IPS), network datasets, cyber security, network topologies, traffic analysis

INTRODUCTION

Intrusion Detection and Prevention Systems (IDS/IPS) have relied on signature matching for much of their history. Signature matching attempts to compare incoming traffic with a library of known attack fingerprints. The main problem with this approach is that it cannot identify threats that have not been catalogued before. Current systems tend to use anomaly-based detection using machine learning and deep learning that can detect zero-day attacks and respond before any damage is done (Khraisat et al., 2019). As detection technology matures, so do the needs for evaluation data and network settings that accurately reflect the operational environment, since experimental results are only meaningful if the test conditions are similar to the networks the systems will eventually protect.

The first wave of intrusion detection system (IDS) research focused on benchmark data sets, notably the KDD Cup 99, which provided comparable performance reference but had duplicated records and traffic that failed to reflect real-life traffic patterns. The main reason why researchers later developed newer datasets, including the UNSW-NB15, CICIDS2017, and Bot-IoT, was to include contemporary attack classes and realistic traffic patterns (Moustafa & Slay, 2015; Sharafaldin et al., 2018; Koroniotis et al., 2019).

Evaluation datasets play a critical role in IDS/IPS research since no intrusion detection model can be better than the data it is trained and tested on. For example, Usman and Kareem (2026) used the NSL-KDD benchmark data set because of its organizational ease, near balance, and clear labels. The researchers reasoned that despite being based on obsolete traffic data, the NSL-KDD was a suitable choice for evaluating modern attack detection models since it remained the standard in cybersecurity research. The NSL-KDD was used to train and test the detection model against the four attack categories of DoS, Probe, U2R, and R2L that overwhelm networks, probe for weaknesses, gain unauthorized root access, and attempt to hijack remote systems, respectively (Usman & Kareem, 2026). Overall, the NSL-KDD set comprised 1,152,281 records, of which 1,074,992 were used for training and 77,289, for testing and validation.

Another rationale for selecting the NSL-KDD was comparability since it enabled the researchers to compare their results with similar studies. However, IDS/IPS benchmark data sets face several challenges that limit the extent to which researchers can generalize their findings. First, researchers rarely use actual traffic data but rely on synthetic or testbed traffic, which may not always reflect actual traffic patterns. Second, network environments are not static, making it difficult to create reliable datasets for IDS evaluation. Third, the field lacks a standardized, universally accepted benchmark dataset, which has resulted in conflicting findings among similar studies (Goldschmidt & Chudá, 2025). These issues help explain the need for evaluating the network and traffic data used to develop intrusion detection systems.

Despite the many improvements in detection and response to network security threats, intrusion detection remains a major challenge for computer networks. Three issues stand out in most IDS evaluations, including the lack of appropriate reference data, the use of obsolete benchmark sets, and differences in evaluation frameworks. Evaluation data were

found to be the most significant limitation in IDS research since most of the datasets used to develop, train, and test detection models were synthetic, not actual traffic data (Goldschmidt & Chudá, 2025). Another limitation was the reliance on old benchmark sets that have been used in IDS research for years despite the numerous improvements in network traffic encryption and attack sophistication. The UNSW-NB15, NSL-KDD, CICIDS2017, and other datasets are no longer useful in detecting modern attacks like DDoS and advanced persistent threats (Moustafa & Slay, 2015; Sharafaldin et al., 2018; Goldschmidt & Chudá, 2025). Finally, the variation in evaluation frameworks makes it unclear if findings are comparable across varying network configurations. For example, models evaluated in one network setup are likely to fail when deployed in different network architectures since they cannot address new threat models (Cantone et al., 2024). Overall, these limitations highlight the need to evaluate the datasets and network settings used in computer network intrusion detection.

Besides data, another critical aspect of IDS/IPS evaluation is the network configuration used to conduct the experiment. For example, Edegbe and Acheme (2024) discuss the difference between centralized and decentralized network configurations and their impact on intrusion detection process. In a centralized system, the server is usually the focal point of all of the network data, which makes it easy to monitor, configure, and manage traffic, but at the same time becomes a primary target for attacks. By contrast, decentralized systems will rather rely on distributed data and processing, with the major advantage of increasing security and resilience to attacks but this requires more robust encryption and authentication mechanisms. The majority of the traffic processing systems of IoT and edge devices have a default network configuration of decentralized systems. The network framework is a crucial determinant for assessing IDS/IPS models, as it specifies the attack surface and general traffic patterns within which intrusion detection models must function. Networks can be categorized by size, purpose and application such as home, school, corporate, mobile, Internet, social and government networks. The various classifications of networks with the features and examples in the real world are shown in figure 1 below.

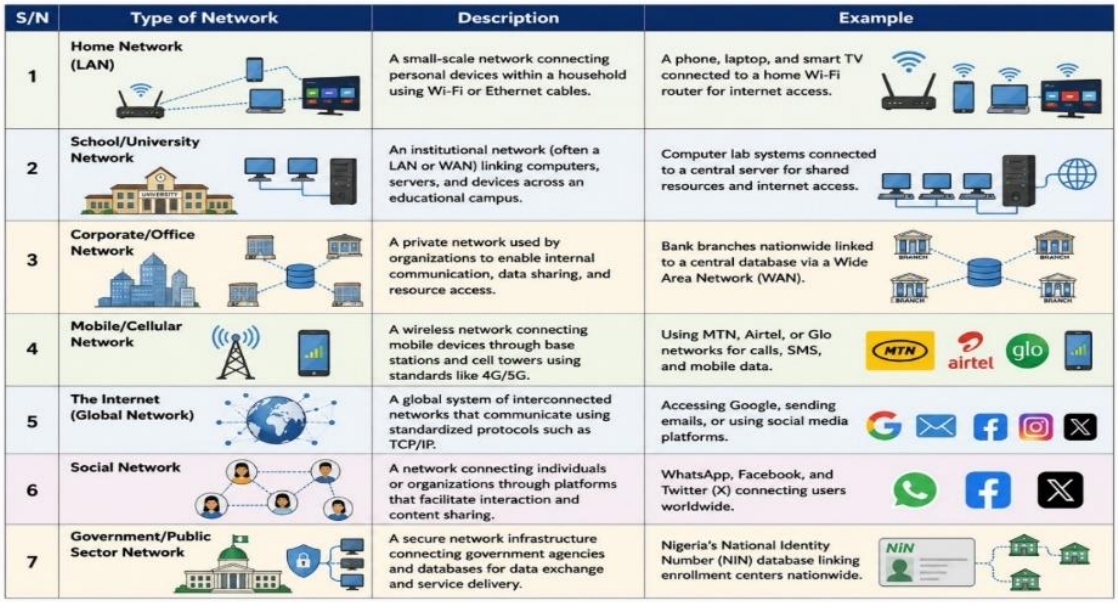

Figure 1: A Visual Overview of Common Real-World Network Types

Real-world networks underpin modern communication by linking devices across settings as varied as households, educational institutions, and organizations. Table 1 lists representative examples of such networks together with brief descriptions.

Table 1: Summary of reviewed studies on Real-World Network Types and Description

S/N	Type of Network	Description	Example	Authors
1	Home Network (LAN)	A small-scale network that connects personal devices within a home using wired (Ethernet) or wireless (Wi-Fi) connections.	A phone, laptop, and smart TV connected to a home Wi-Fi router for internet access.	Forouzan (2013); Kurose & Ross (2021)
2	School/University Network	An institutional network that connects computers, servers, and other devices across a school or university campus to enable communication and resource sharing.	Computer laboratory systems connected to a central server for file sharing and internet access.	Tanenbaum & Wetherall (2011); Stallings (2022)
3	Corporate/Office Network	A private network used by organizations to support communication, data sharing, and access to business applications across departments or branches.	Bank branches connected to a central database through a Wide Area Network (WAN).	Stallings (2022); Kurose & Ross (2021)
4	Mobile/Cellular Network	A wireless communication network that connects mobile devices through cellular base stations using technologies such as 4G LTE and 5G.	Using MTN, Airtel, or Glo networks for voice calls, SMS, and mobile internet services.	Dahlman, Parkvall, & Sköld (2021)

S/N	Type of Network	Description	Example	Authors
5	Internet (Global Network)	A worldwide network of interconnected computer networks that communicate using the TCP/IP protocol suite.	Browsing Google, sending emails, or accessing cloud services.	Kurose & Ross (2021); Tanenbaum & Wetherall (2011)
6	Social Network	An online platform that enables individuals or organizations to communicate, collaborate, and share digital content.	WhatsApp, Facebook, Instagram, and X (formerly Twitter).	Boyd & Ellison (2007); Kaplan & Haenlein (2010)
7	Government/Public Sector Network	A secure network infrastructure used by government agencies to exchange information, provide public services, and manage national databases.	Nigeria's National Identity Number (NIN) database connecting enrollment centres across the country.	Stallings (2022); Kurose & Ross (2021)

This study is mainly focused on carrying out a comparison of network environments and benchmark datasets that have been used over the years for Intrusion Detection and Prevention System (IDS/IPS). The study has three objectives, these are; to review the network environments used for IDS/IPS evaluation and analyze their characteristics and performance assessment capabilities. Two, to identify and compare the publicly available benchmark datasets and assess their feature sets, attack coverage, and applicability. Finally, to highlight the limitations and gaps in the existing network environments and datasets, as well as identify the appropriate datasets for future development and evaluation endeavors of IDS/IPSs.

In order to achieve this the following research questions were formulated: What are common categories of the network environment used in the evaluation of the Intrusion Detection and Prevention System (IDS/IPS) and to what extent could this environment type support the assessment of detection capabilities? What are the characteristics, attack coverage, and applicability of the publicly available datasets for research needs? What are the gaps and limitations of the existing environments and datasets, and which of the available datasets could be considered as the best option for future evaluations? The objectives directly correlate with the three research questions above. Indeed, each of the research questions was developed to explicitly address one of the objectives. Therefore, the combination of questions and objectives allows for conducting a comprehensive comparative analysis of the IDS/IPS test environments and benchmark datasets, identifying their strengths and weaknesses and providing evidence-based recommendations. Evaluation environments of IDS/IPSs could be generally categorized based on the underlying infrastructure and operation principles. Specifically, the network environments utilized for IDS/IPS assessment could be generally grouped into simulated, live traffic, lab-based, cloud- and IoT-based environments. These network environments differ by a range of factors including realism, levels of control, scalability, and other parameters, which affect the accuracy and generalizability of results across various network environments. Figure 2 below presents the main types of network environment utilized for the assessment of IDS/IPS.

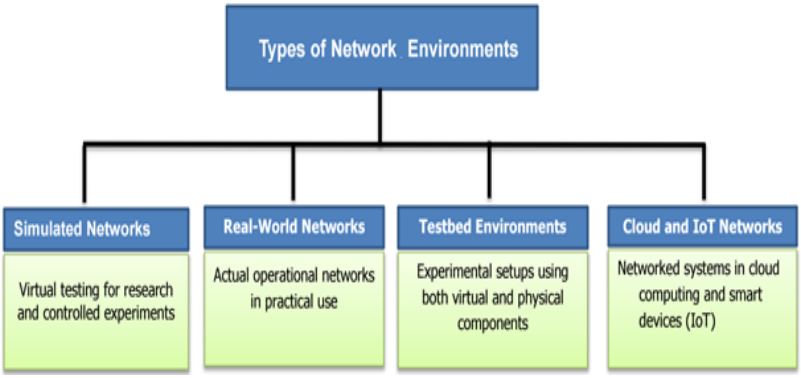

Figure 2: Classification of Network Environments Used in IDS/IPS Evaluation

Reliable IDS/IPS assessment is possible only by using realistic and diverse data for testing. Early databases such as DARPA98, KDD Cup 99, NSL-KDD, and others have been widely recognized for their limitations in terms of obsolete attack types, data duplication, and traffic inconsistency with modern networks. Later, researchers proposed new datasets including UNSW-NB15, CICIDS2017, CSE-CIC-IDS2018, TON_IoT, Edge-IIoTset, etc. Goldschmidt and Chudá (2025) have analyzed 89 intrusion detection publicly available datasets in their survey, revealing a significant number of publications related to the creation of data sets since 2020. Moreover, the authors have identified multiple issues related to artificial traffic, insufficient realism, imbalanced classes, incorrect labeling, and lack of coverage of current attack types. While CICIDS2017 is the most widely used database, it comprises less than a third of all studies, indicating that the scientific community lacks consensus on the standard test data and that a choice should be guided by specific goals.

Pinto et al. (2025) have noticed that increased interest in machine learning and deep learning technologies has led to a growing demand for high-quality data sets, while many popular databases, including the CIC family of data sets, have inconsistencies, incorrect labeling, and imbalanced attack distributions. Researchers have also raised concerns about the reliance on CICFlowMeter and other traffic-extraction utilities and pointed out that these shortcomings undermine the reliability of comparisons between intrusion detection methods. Similar conclusions can be drawn from the reviews by Goldschmidt and Chudá (2025) and Pinto et al. (2025). They revealed that the most popular data sets for machine learning-based intrusion detection are CICIDS2017, CSE-CIC-IDS2018, UNSW-NB15, NSL-KDD, which provide standardized traffic, a wide range of attack classes, and an open-source community. However, none of these data sets accurately represent the heterogeneous environments of

enterprise, cloud, IoT, industrial, and software-defined networks.

Therefore, most researchers now prefer to use multiple benchmark data sets to assess the performance of detection and prevention models on different networks. Moreover, there is a tendency to move from pure classification accuracy to a more realistic assessment of the adequacy of these data sets for specific industries. Rahman Tori and Hasan (2026) have proposed a multi-criteria assessment framework that focuses on the correspondence of data sets to the MITER ATT&CK knowledge base and industry context, thereby highlighting the importance of taking into account the application-specific aspects of attack types, intrusion detection models, and networks when choosing data sets for research. The authors showed that even the most recent publicly available databases contain few records covering critical sectors such as healthcare, finance, and energy. Therefore, an empirical assessment of the usefulness of data sets should also include an analysis of network environments and existing benchmarks. This fact, along with the findings of other surveys, indicates that future studies on intrusion detection/prevention systems should focus on network-specific aspects as a key factor influencing detection accuracy, the choice of data sets, and the reliability of comparisons between emerging technologies.

MATERIALS AND METHODS

To conduct this survey, relevant journal articles and conference papers that describe network environments and benchmark data sets for intrusion detection and prevention systems were retrieved from databases including IEEE Xplore, ACM, Springer, ScienceDirect, Google Scholar, and others. Whenever possible, articles published in the last 16 years (2009-2026) were selected, along with original research on intrusion detection systems benchmark data sets, including early KDD Cup 99, NSL-KDD, and other related topics. Studies on intrusion detection/prevention system benchmark datasets were identified, and the following details were specifically extracted: type of network environment, source of traffic, attack classes, number of features, dataset size, labeling method, and strengths and weaknesses described by the authors. The network environments included enterprise, cloud, IoT, IIoT, Software Defined Networks (SDN), and hybrid.

The extracted information was organized into tables and analyzed to identify trends and research gaps. Benchmark datasets were evaluated based on realism, attack class coverage, host network environment, feature set richness, and scalability, among other factors related to modern intrusion detection/prevention system needs and machine learning capabilities. The findings were then compiled into this manuscript, which contains concluding remarks and recommendations. This study can be reproduced by following the provided methodology, which includes iterative procedures for researching and analyzing scientific literature on intrusion detection/prevention system network environments and benchmark data sets.

RESULTS AND DISCUSSION

The results of the survey are presented in this section, divided into network environments used to evaluate intrusion detection/prevention systems, the benchmark datasets derived from them, and the strengths, weaknesses, and research gaps identified in this study. These findings are summarized in tables followed by a discussion of their importance to intrusion detection/prevention system research.

Comparison of Network Environments used for IDS/IPS Evaluation

The network environments described in the selected articles were grouped into real, simulated, and emulated (Table 2). The primary characteristics, benefits, drawbacks, and references are described. As seen in the table, the debate between authenticity and simplicity dominates the discussion of network environments. Thus, real-time networks provide a rich and authentic experience, while simulated networks offer excellent flexibility and control.

Table 2: Comparison of Network Environments Employed in IDS/IPS Evaluation

Environment Type	Key Characteristics	Advantages	Limitations
Operational production networks	Traffic captured from live enterprise, cloud, ISP, campus, or data center networks featuring diverse users, devices, applications, and protocols	Maximum realism; reflects genuine user behavior, encrypted flows, background noise, and evolving attack patterns	Hard to acquire owing to privacy, confidentiality, and legal constraints, together with the expense of accurate labeling (Goldschmidt & Chudá, 2025)
Simulated networks	Traffic and attacks produced inside software simulators (e.g., NS-3, OMNeT++) under fixed configurations	Inexpensive, repeatable, tightly controllable, and well suited to studying particular attack types	Cannot fully recreate the complexity, variability, and unpredictability of live traffic, which can inflate reported performance (Sharafaldin et al., 2018)
Emulated/Testbed networks	Physical or virtual laboratory setups running genuine protocols, applications, and attacks under controlled conditions	Strike a balance between realism and control; enable repeatable testing of enterprise, cloud, and IoT security solutions	Smaller scale, narrower diversity, and less authentic user behavior than production networks, limiting how fully they represent operational settings (Koroniotis et al., 2019; Goldschmidt & Chudá, 2025)
Publicly available benchmark datasets	Ready-made, labeled traffic collections (e.g., NSL-KDD, CICIDS2017, UNSW-NB15) built in simulated or emulated settings and published for offline testing	Permit standardized, repeatable comparison of IDS/IPS models across studies; broad adoption saves time and cost	Frequently dated, class-imbalanced, or marked by artifacts of the original capture setting, which weakens generalization to present threats (Sharafaldin et al., 2018)
Hybrid networks	Genuine background traffic from production networks blended with injected or synthetic attack flows	More realistic than pure simulation while preserving a degree of control over attack labeling	Merging real and synthetic flows can create mismatched traffic characteristics that bias results (Goldschmidt & Chudá, 2025)

Table 2 straightaway shows that for all IDS/IPS evaluation criteria, a universal environment proved elusive. Real-life traffic proved the most accurate but also the hardest to come by, whereas the use of simulations and emulations was

convenient but produced only approximate results. Thirmuran et al. (2024) and Rani et al. (2023) reported that systems tested against mixed traffic differed in their responses to real traffic, an observation that highlighted the danger of extrapolating lab-based findings to operational settings.

Comparison of Benchmark Datasets used for IDS/IPS Evaluation

Table 3 compares the five benchmark datasets used in the reviewed articles in terms of the year of publication, type of network environment, traffic generation methodology, variety of attacks, and known limitations. The table is directly informative for the current research since it enables an evidence-based assessment of how realistic and representative these datasets are of modern networks.

Table 3: Comparative Summary of Benchmark Datasets in IDS/IPS Research

Dataset	Year	Network Context	Traffic Generation	Attack Coverage	Key Limitations
KDD Cup 99	1999	Simulated U.S. Air Force LAN	Fully simulated traffic	DoS, Probe, R2L, U2R	Redundant records, heavy class imbalance, and obsolete attack profiles (Tavallaee et al., 2009).
NSL-KDD	2009	Refined version of KDD Cup 99	Derived from KDD Cup 99 with duplicate records removed	DoS, Probe, R2L, U2R	Removes duplication yet still reflects legacy attacks and dated traffic behavior (Tavallaee et al., 2009).
UNSW-NB15	2015	Hybrid enterprise network	Hybrid traffic produced with the IXIA PerfectStorm tool, mixing legitimate flows with synthetic attacks	Nine contemporary attack families	Weak coverage of genuinely operational network traffic (Moustafa & Slay, 2015).
CICIDS2017	2017	Enterprise network testbed	Lifelike benign traffic paired with modern attack types	Brute Force, DoS, DDoS, Web attacks, Botnet, Infiltration, Port Scan	Oriented toward enterprise settings and only partially reflects cloud or IoT contexts (Sharafaldin et al., 2018).
Bot-IoT	2019	IoT cyber range	Simulated IoT flows featuring credible botnet attack types	DDoS, DoS, reconnaissance, information theft, and botnet attacks	Built chiefly for IoT contexts and less appropriate for enterprise IDS/IPS testing (Koroniotis et al., 2019).

Whereas KDD Cup 99 does contain simple traffic, later sets, including CICIDS2017 and Bot-IoT, include more diverse traffic. At the same time, KDD Cup 99 and NSL-KDD are still widely used because they are easily accessible and well-researched. Thus, less biased data sets have much lower popularity among researchers, leading to a gap between available resources and actual usage.

Trade-off between Comparability and Realism

It was revealed that there was a frequent dilemma between using old data sets, which allows easier comparisons of results, and recent ones, which better represent current networks. The trade-off between these two aspects is presented in Table 4 below, which also highlights some advantages and disadvantages of the discussed sets.

Table 4: Comparability Realism Trade-off: Legacy vs. Modern Benchmark Datasets

Criterion	Legacy Datasets (KDD Cup 99, NSL-KDD)	Modern Datasets (UNSW-NB15, CICIDS2017, Bot-IoT)
Cross-study comparability	High: long-standing benchmarks that have supported consistent comparison and reproducibility across IDS studies (Tavallaee et al., 2009)	Moderate: frequently used in recent work, though none has attained universal benchmark standing (Goldschmidt & Chudá, 2025)
Ecological validity	Low: realism is constrained by dated traffic and attack profiles (Tavallaee et al., 2009)	Higher: broader attack diversity and more credible background traffic, though most collections are still testbed-derived (Sharafaldin et al., 2018; Goldschmidt & Chudá, 2025)
Relevance to current cyber threats	Low: poorly reflects current attack techniques and emerging threat landscapes (Tavallaee et al., 2009)	High: covers present-day categories including web attacks, botnets, DDoS, and IoT-specific threats (Moustafa & Slay, 2015; Koroniotis et al., 2019)
Deployment relevance	Chiefly fit for controlled laboratory experiments in generic network settings (Tavallaee et al., 2009)	Closer to enterprise, cloud, and IoT conditions, yet still constrained by reliance on laboratory or testbed traffic (Goldschmidt & Chudá, 2025)

As Table 4 indicates, neither dataset generation can claim outright superiority under objective assessment. The significance of this observation is that it recasts dataset selection as a context-sensitive methodological judgement rather than a binary choice between an obsolete and an updated option. Researchers whose priority is comparability with the accumulated literature may defensibly retain legacy datasets, provided their limitations are stated openly, while those prioritizing realism and threat currency are better served by modern, domain-specific alternatives despite their thinner record of cross-study adoption.

Summary of Research Trends and Gaps

Table 5 draws together the main trends observed in the reviewed literature, the research gaps attached to each, and the implications these carry for the design of future studies.

Table 5: Summary of Identified Trends and Corresponding Research Gaps

Observed Trend	Associated Research Gap	Implication for Future Research
Persistent reliance on legacy datasets such as KDD Cup 99 and NSL-KDD for IDS evaluation	Dependence on dated traffic and attack representations curtails the realism and generalizability of findings (Tavallaee et al., 2009)	Dataset choices should be defended on grounds of realism, attack diversity, and current-threat relevance, not historical popularity alone
Growing uptake of UNSW-NB15, CICIDS2017, and Bot-IoT without any universally endorsed benchmark	The absence of standard benchmarks hinders fair cross-study comparison of IDS/IPS performance (Moustafa & Slay, 2015; Sharafaldin et al., 2018; Goldschmidt & Chudá, 2025)	New methods should be tested on several complementary benchmark datasets to strengthen comparability and generalizability
Ongoing reliance on synthetic or testbed traffic when constructing datasets	Ecological validity suffers because laboratory traffic cannot reproduce the full complexity and variability of live networks (Goldschmidt & Chudá, 2025)	Build hybrid datasets pairing authentic operational traffic with controlled attack types while safeguarding reproducibility
IDS evaluations are carried out largely in controlled laboratory or testbed settings	Scant evidence exists on IDS/IPS effectiveness in production-scale enterprise, cloud, and IoT networks (Koroniotis et al., 2019)	Expand validation in operational or near-production networks to gauge deployment performance more accurately
Few publicly available datasets contain genuine operational network traffic	Privacy, legal, confidentiality, and labeling barriers impede the collection and sharing of real-world security data (Goldschmidt & Chudá, 2025)	Explore privacy-preserving sharing mechanisms such as anonymization, synthetic data augmentation, federated learning, and federated evaluation to enable secure collaboration without exposing sensitive network data

Viewed as a whole, Tables 1 through 5 supply an evidence-driven and repeatable comparison of the environments and benchmarks used in IDS/IPS evaluation, cataloguing their properties, merits, shortcomings, and bearing on current cybersecurity research. They show that although increasingly realistic and domain-tailored evaluation resources have been produced, their uptake trails their availability, and testing practice remains weighted toward controlled, simulated settings at the cost of ecological validity. This pattern supports the central contention of the review: a durable gap separates benchmark conditions from the complexity of live networks, and narrowing it will demand deliberate, criteria-led selection of datasets and environments rather than continued deference to legacy convention.

CONCLUSION

This review found that older datasets and simulated test settings retain their popularity chiefly because they are readily accessible and permit straightforward comparison with earlier work. Useful as they are, such resources capture only a fraction of the conditions present in contemporary networks, so the IDS/IPS performance figures reported in much of the literature are likely to overstate what the same models would achieve in deployment. Live networks mix heterogeneous traffic, shifting user behavior, and novel attack techniques that older datasets and controlled simulations seldom represent. Future studies should therefore lean more heavily on recent datasets and more faithful test environments, and blending simulated traffic with genuine or recorded captures offers one practical route to more dependable evaluation. Pursuing this direction will support the development of IDS/IPS models that are genuinely ready for deployment in real network environments.

REFERENCES

Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication, 13(1), 210–230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

Cantone, M., Marrocco, C., & Bria, A. (2024). On the cross-dataset generalization of machine learning for network intrusion detection. IEEE Access, 12, 144489–144508. https://doi.org/10.1109/ACCESS.2024.3472907

Dahlman, E., Parkvall, S., & Sköld, J. (2021). 5G NR: The next generation wireless access technology (2nd ed.). Academic Press.

Edegbe, G. N., & Acheme, S. (2024). A systematic review of centralized and decentralized machine learning models: Security concerns, defenses and future directions. NIPES Journal of Science and Technology Research, 6(4), 161–175. https://doi.org/10.5281/zenodo.14681449

Forouzan, B. A. (2013). Data communications and networking (5th ed.). McGraw-Hill Education.

Goldschmidt, P., & Chudá, D. (2025). Network intrusion datasets: A survey, limitations, and recommendations. Computers & Security, 156, 104510. https://doi.org/10.1016/j.cose.2025.104510

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. Business Horizons, 53(1), 59–68. https://doi.org/10.1016/j.bushor.2009.09.003

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. Cybersecurity, 2, Article 20. https://doi.org/10.1186/s42400-019-0038-7

Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2019). Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. Future Generation Computer Systems, 100, 779–796. https://doi.org/10.1016/j.future.2019.05.041

Kurose, J. F., & Ross, K. W. (2021). Computer networking: A top-down approach (8th ed.). Pearson.

Martins, et al. (2025). Adaptive online learning approaches for detecting unknown attacks in network traffic: A systematic literature review. Security and Privacy.

Moustafa, N., & Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In 2015 Military Communications and Information Systems Conference

(MilCIS) (pp. 1–6). IEEE. https://doi.org/10.1109/MilCIS.2015.7348942

Pinto, D., Amorim, I., Maia, E., & Praça, I. (2025). A review on intrusion detection datasets: Tools, processes, and features. Computer Networks, 262, 111177.

Rahman Tori, A., & Hasan, K. F. (2026). An evaluation framework for network IDS/IPS datasets: Leveraging MITRE ATT&CK and industry relevance metrics. Computers & Security, 161, 104777.

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. In Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018) (pp. 108–116). SciTePress. https://doi.org/10.5220/0006639801080116

Stallings, W. (2022). Data and computer communications (11th ed.). Pearson.

Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer networks (5th ed.). Pearson.

Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. In 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications (pp. 1–6). IEEE. https://doi.org/10.1109/CISDA.2009.5356528

Thirumaran, V., Joseph, N., & Srikanth, G. (2024). Intrusion detection system in cloud computing using VTR-HLSTM-based deep learning. Indonesian Journal of Electrical Engineering and Computer Science, 33(3), 1829–1842. https://doi.org/10.11591/ijeecs.v33.i3.pp1829-1842

Usman, O. L., & Kareem, M. A. (2026). An intrusion detection system based on hybridized firefly and artificial bee colony optimization algorithms. FUDMA Journal of Sciences, 10(ANB-K Special Issue), 40–47. https://doi.org/10.33003/fjs-2026-10(ANB-K)-5306