© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1722869

Machine Learning Techniques for Intrusion Detection Systems in 5G and Beyond Networks: A Systematic Literature Review

ELIJAH ABAYOMI OLANIYI[1], TEMITOPE OLUFUNMI ATOYEBI[2], RIDWAN KOLAPO[3], PREMA A. KIRUBAKARAN[4]

[1,2,3,4]*Department of Information Technology, Faculty of Computing, Nile University of Nigeria. Abuja, Nigeria.*

Abstract- ***5G and subsequent network systems are designed with a number of these features like super-fast data transfer, ultra-low latency, huge number of connections, cloud network, multi-access edge computing, and network function virtualization. But also, they are the primary cause of the proliferation of cyber-attacks and the evolution of intelligent intrusion detection system. The manuscript describes a comprehensive review of the literature concerning the application of machine learning to intrusions detection systems in 5G and beyond networks. The survey includes various kinds of models, datasets, categories of attack, validation methods, assessment metrics, deployment readiness, explainability and privacy considerations. Studies published between 2020 and 2026 were examined using PRISMA-guided selection and structured data extraction method. Findings from 21 reviewed studies show that empirical ML/DL evaluation studies accounted for 42.9%, review or survey syntheses accounted for 23.8%, federated or transfer learning studies accounted for 19.0%, and dataset/testbed studies accounted for 14.3%. Representative benchmark accuracies ranged from 64.1% for application-layer PFCP detection to 100.0% for binary 5G-NIDD classification. The paper concludes that no single model is universally best; rather, technique selection should depend on the type of attack, the quality of validation, the amount of latency, the scalability, privacy, and explainability, to determine the most appropriate approach.***

Keywords- ***5G Security, Beyond 5G, Intrusion Detection System, Machine Learning, Deep Learning, Federated Learning, PRISMA, and Systematic Literature Review.***

I. INTRODUCTION

Fifth generation (5G) and beyond networks reinforces enhanced mobile broadband, ultra-reliable low-latency communication, massive machine-type communication, software-defined networking, network function virtualization, network slicing and multi-access edge computing [1], [2]. These capabilities trigger a wide range of emerging applications such as smart cities, industrial automation, autonomous systems, telemedicine and large-scale Internet of Things deployment, but this development also introduce greater complexity of securing modern communication infrastructures.

5G and beyond networks have a much larger attack surface compared to earlier mobile generations since as security monitoring it must include also radio access components, cloud-native core functions, control-plane interfaces, edge nodes, virtualized network functions, orchestration platforms, application programming interfaces and network slices [2], [7]. These threats are: denial of service, distributed denial of service, spoofing, scanning, botnet activity, malware propagation, unauthorized access, signaling abuse, data exfiltration and adversarial manipulation of AI-based systems [2], [19, 22].

Intrusion Detection Systems (IDS) are required to identify rogue traffic, suspicious activity, policy violations and anomalous patterns before they compromise confidentiality, integrity and availability. Traditional signature-based systems remain useful for known threats, but anomaly-based and machine-learning-based IDS are increasingly important because they can learn from network traffic, logs and telemetry and detect attacks that may not have fixed signatures [3], [4].

Although many studies report strong machine learning performance for IDS, the evidence base for 5G and beyond networks remains fragmented across datasets, model families, validation strategies, attack categories and operational assumptions. This paper therefore reviews, classifies and synthesizes machine learning techniques for IDS in 5G and beyond networks, with attention to dataset realism, validation credibility, deployment readiness, explainability and privacy.

II. LITERATURE REVIEW

A. 5G/B5G IDS Context

5G and beyond networks introduce service-based core architecture, network slicing, SDN, NFV and MEC. These technologies improve flexibility and latency, but they also create additional points at which intrusions may occur [1], [2]. In this context, IDS can be deployed at the RAN, 5G core, MEC, SDN controller, virtualized function layer, slice manager or IoT gateway [4], [17].

Research on datasets shows that general-purpose intrusion datasets such as UNSW-NB15 and CICIDS2017 remain useful for baseline comparison, but they do not fully represent 5G service-based core interfaces, O-RAN telemetry, MEC or network slicing [20-22]. Recent datasets and testbeds such as 5G-NIDD, PFCP/5G core datasets and O-RAN KPI datasets improve relevance, although each still covers only part of the 5G ecosystem [6]-[9].

B. Machine Learning Techniques

The use of classical ML techniques in IDS has not reduced the significance of them because many of the datasets associated with networks remain to be tabular or flow-based. Decision trees, Random forests, Extra trees, Gradient boosting and XGBoost are the commonly mentioned ones because they are the best for non-linear correlation and can do feature-importance analysis [5], [12], [13]. SVM, KNN, Naive Bayes and Logistic Regression are also the alternative paths for some particularly simple and computationally efficient situations [12], [18].

When complex spatial, temporal or latent traffic patterns exist, deep learning methods like CNN, LSTM, GRU, auto encoder and hybrid CNN-LSTM models are used [3], [14]. Transfer learning is a technique that allows adaptation to the situation when the labeled 5G attack data are scarce while federated learning is the framework that preserves privacy by enabling a collaborative training on across devices edge nodes or operators [15], [16] Security analysts, particularly those working in operational 5G core or edge environments, require understandable alerts that is why explainable AI also holds importance [13].

III. METHODOLOGY

The systematic literature review design as shown in Table 1 below was used in the study because the main goal was to identify, evaluate, and synthesize the available published evidence instead of gathering the primary network traffic or implementing a new IDS prototype. The review was guided by PRISMA 2020 reporting principles and software engineering systematic review guidance [10], [11].

Searches covered IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, Scopus, Web of Science, MDPI, Frontiers, Google Scholar and selected dataset repositories. The search combined terms for network generation, detection task and learning method, including: 5G, beyond 5G, 6G, network slicing, MEC, O-RAN, intrusion detection, anomaly detection, machine learning, deep learning, federated learning, transfer learning and explainable AI.

The studies accessed are the ones that were accepted between 2020 and 2026, written in English, are available in full text, focus on IDS or anomaly detection in 5G/B5G/6G or directly related enabling networks, and provide relevant evidence on machine learning technique, dataset, attack type, metric or review finding. The studies not included in the process were those that did not fit in the IDS scope, those lacking a method, those being duplicate records, or those that were from non-scholarly sources.

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1722869

Table I: Objective vs Methodology Matching

Objective	Methodology	Expected Result
Objective 1	Systematic search and technique classification	Taxonomy of ML, DL, TL, FL and XAI techniques
Objective 2	Dataset, domain and metric extraction	Dataset/testbed and evaluation summary
Objective 3	Narrative and thematic synthesis	Strengths, weaknesses and performance patterns
Objective 4	Gap analysis and taxonomy mapping	Research agenda and deployment-aware recommendations

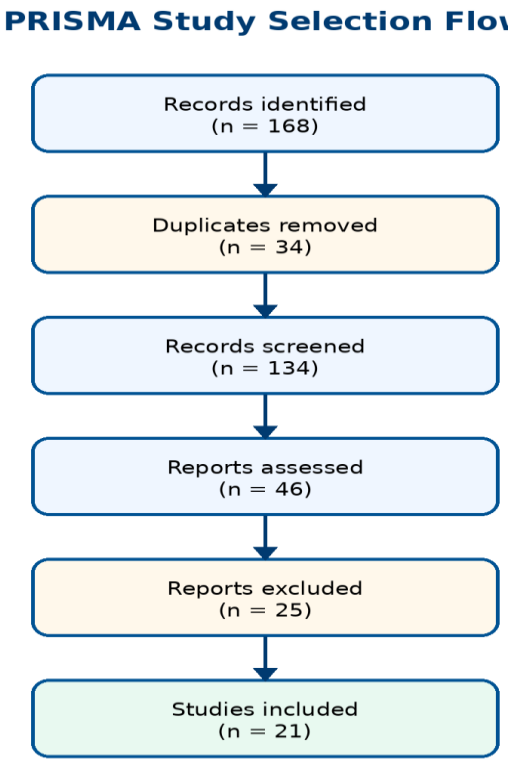

Figure 1: PRISMA Study Selection Flow

IV. RESULTS AND DISCUSSIONS

The PRISMA screening record as displayed in Figure 1 commenced with 168 records identified from databases and registers. After removing 34 duplicate records, 134 records proceeded to screening. Forty-six reports were reevaluated for eligibility, 25 reports were excluded with documented reasons, ultimately 21 studies met the inclusion criteria and were selected for the final synthesis. The step-by-step following of the selection procedure, as the scientific method indicates, not only enhanced the visibility but also made the study population more homogeneous and the arbitrary inclusion could be considerably curbed [11].

The scrutinized papers state that classical machine learning, deep learning, transfer learning, federated learning, and explainable AI are the principal approaches to IDS in 5G and future networks. Yet, the optimum method is conditioned by the data source, attack class, validation procedure, and

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1722869

deployment restriction. That being the case, this review aims at no models only by accuracy but also interprets the outcome with respect to dataset realism, leakage control, class imbalance, false alarms, latency, scalability, privacy, and explainability.

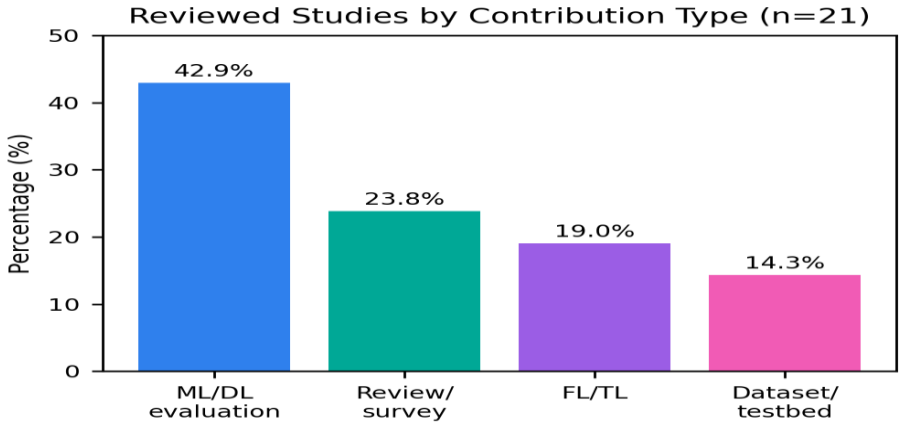

Figure 2: Reviewed Studies by Primary Contribution

The chart presented in Figure 2 indicates that empirical ML/DL studies are the most common type, representing 42.9% of the total 21 studies assessed. They are followed by review or survey syntheses that are 23.8% of the total number, federated or transfer learning studies making up 19.0%, and dataset/testbed studies representing 14.3%. These numbers reveal the fact that the debate between empirical and synthesis offering is half experimental and half theoretical. However, it is true that the type of evidence-oriented data-resource studies in the literature is smaller by comparison.

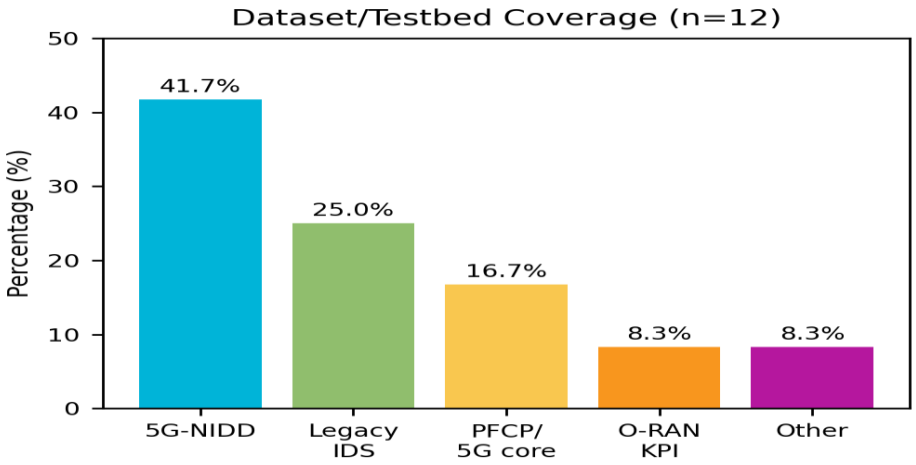

Figure 3: Dataset/Testbed Coverage in Empirical Studies

Figure 3 shows that 5G-NIDD was the most frequent 5G-oriented data resource among the empirical and data-resource studies, representing 41.7% of the 12 studies in this breakdown. Legacy IDS datasets accounted for 25.0%, PFCP/5G core datasets accounted for 16.7%, and O-RAN KPI and other 5G/private testbeds each accounted for 8.3%. This supports the finding that 5G realism is improving, but still uneven across network domains.

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1722869

Table II: Recommended Technique Selection Matrix

IDS Scenario	Best Technique	Reason
Tabular flow IDS	RF, Extra Trees, GB, XGBoost	Strong structured-data baseline [5], [12], [13]
5G-NIDD benchmark	KNN / Voting Classifier	Strong accuracy, ROC AUC and F1 [12], [18]
Complex or scarce data	DL / Deep Transfer Learning	Learns complex patterns and adapts labels [14], [15]
Privacy and trust	FL + XAI	Supports distributed learning and explanations [13], [16]

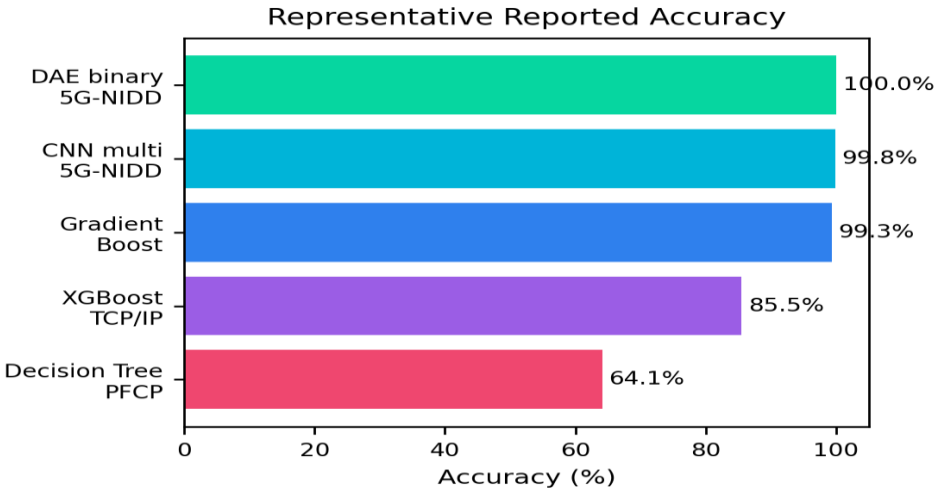

Figure 4: Representative Accuracy Results Reported in Selected Studies

Representative metrics show that reported performance varies by dataset and feature representation as reflected in Table II and III. [14] reported 100.0% accuracy, precision, recall and F1-score for binary 5G-NIDD classification with a dense auto encoder, and 99.84% accuracy, 99.84% precision, 99.83% recall and 99.84% F1-score for multi-class CNN classification. [5] reported 99.3% accuracy for Gradient Boost in a secure-data test and 96.4% on the attack test set. [13] mentioned that 85.5% accuracy and 85.4% F1-score for XGBoost using TCP/IP flow statistics, but 64.1% accuracy and 64.2% F1-score for Decision Tree using application-layer PFCP statistics as shown in Figure 4. These values show that very high performance is possible, but performance claims must be interpreted with regard to the dataset, protocol layer, attack coverage and validation method.

Table III: Main Gaps and Research Implications

Gap Area	Implication for 5G/B5G IDS
Dataset realism	More datasets are needed for slicing, MEC, signaling, APIs and insider threats.
Validation credibility	Leakage-free splitting, imbalance handling and external validation should be reported.
Deployment readiness	Latency, overhead, scalability and update strategy should be evaluated.
Explainability	XAI should be used to support analyst trust and alert interpretation.
Privacy and federation	FL needs poisoning defenses, robust aggregation and communication-cost evaluation.
Reproducibility	Code, parameters, preprocessing and data splits should be disclosed.

V. CONCLUSION

This paper reviewed machine learning techniques for Intrusion Detection Systems in 5G and beyond networks. The review confirms that machine learning is valuable for adaptive intrusion detection, but model choice must be evidence-based and context-aware. A model should not be selected solely because it reports high accuracy; it should also be assessed using dataset realism, leakage control, class imbalance, false positive behavior, latency, scalability, privacy, explainability and robustness.

The strongest practical baseline for tabular flow-based 5G/B5G IDS is tree-based ensemble or boosting, including Random Forest, Extra Trees, Gradient Boosting and XGBoost. KNN and voting classifiers are competitive for 5G-NIDD benchmarking, deep learning is suitable for complex traffic patterns, transfer learning is useful where target-domain labels are limited, and federated learning is suitable for privacy-sensitive distributed environments. Future research should prioritize realistic 5G/B5G datasets, leakage-free evaluation, deployment metrics, explainable models, adversarial robustness and reproducible experimental pipelines.

REFERENCES

[1] 3rd Generation Partnership Project, “3GPP TS 33.501 V18.10.0: Security architecture and procedures for 5G system,” ETSI, 2025.

[2] European Union Agency for Cybersecurity, “ENISA threat landscape for 5G networks,” ENISA, 2020.

[3] A. Aldweesh, A. Derhab, and A. Z. Emam, “Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues,” Knowledge-Based Systems, vol. 189, 105124, 2020, doi: 10.1016/j.knosys.2019.105124.

[4] P. Dini, A. Elhanashi, A. Begni, S. Saponara, Q. Zheng, and K. Gasmi, “Overview on intrusion detection systems design exploiting machine learning for networking cybersecurity,” Applied Sciences, vol. 13, no. 13, 7507, 2023, doi: 10.3390/app13137507.

[5] A. Imanbayev, S. Tynymbayev, R. Odarchenko, S. Gnatyuk, R. Berdibayev, A. Baikenov, and N. Kaniyeva, “Research of machine learning algorithms for the development of intrusion detection systems in 5G mobile networks and beyond,” Sensors, vol. 22, no. 24, 9957, 2022, doi: 10.3390/s22249957.

[6] S. Samarakoon, Y. Siriwardhana, P. Porambage, M. Liyanage, S.-Y. Chang, J. Kim, J. Kim, and M. Ylianttila, “5G-NIDD: A comprehensive network intrusion detection dataset generated over 5G wireless network,” arXiv, 2022, doi: 10.48550/arXiv.2212.01298.

G. Amponis, P. Radoglou-Grammatikis, G. Nakas, S. Goudos, V. Argyriou, T. Lagkas, and P. Sarigiannidis, “5G core PFCP intrusion detection dataset,” in Proc. 12th International Conference on Modern Circuits and Systems Technologies (MOCAST), 2023, pp. 1-4, doi: 10.1109/MOCAST57943.2023.10176693.

[7] P. V. A. Alves et al., “Machine learning applied to anomaly detection on 5G O-RAN architecture,” Procedia Computer Science, vol. 222, pp. 81-93, 2023, doi: 10.1016/j.procs.2023.08.146.

[8] Y. Siriwardhana et al., “Descriptor: 5G wireless network intrusion detection dataset (5G-NIDD),” IEEE Data Descriptions, vol. 2, pp. 358-369, 2025, doi: 10.1109/IEEEDATA.2025.3592888.

[9] B. Kitchenham and S. Charters, “Guidelines for performing systematic literature reviews in software engineering,” EBSE Technical Report EBSE-2007-01, Keele University and Durham University, 2007.

[10] M. J. Page et al., “The PRISMA 2020 statement: An updated guideline for reporting systematic reviews,” BMJ, vol. 372, n71, 2021, doi: 10.1136/bmj.n71.

[11] M. A. Bouke and A. Abdullah, “An empirical assessment of ML models for 5G network intrusion detection: A data leakage-free approach,” e-Prime - Advances in Electrical Engineering, Electronics and Energy, vol. 8, 100590, 2024, doi: 10.1016/j.prime.2024.100590.

[12] P. Radoglou-Grammatikis et al., "5GCIDS: An intrusion detection system for 5G core with AI and explainability mechanisms," in Proc. IEEE Globecom Workshops, 2023, pp. 353-358, doi: 10.1109/GCWkshps58843.2023.10464667.

[13] A. Moubayed, "A complete EDA and DL pipeline for softwarized 5G network intrusion detection," Future Internet, vol. 16, no. 9, 331, 2024, doi: 10.3390/fi16090331.

[14] B. Farzaneh, N. Shahriar, A. H. Al Muktadir, M. S. Towhid, and M. S. Khosravani, "DTL-5G: Deep transfer learning-based DDoS attack detection in 5G and beyond networks," Computer Communications, vol. 228, 107927, 2024, doi: 10.1016/j.comcom.2024.107927.

[15] H. Rezaei, R. Taheri, E. Nowroozi, M. Hajizadeh, S. Shiaeles, and T. Bauschert, "A survey on security and privacy in federated learning-based intrusion detection systems for 5G and beyond networks," IEEE Open Journal of the Communications Society, vol. 7, pp. 253-300, 2025, doi: 10.1109/OJCOMS.2025.3644477.

[16] C. Hamroun, A. Fladenmuller, M. Pariente, and G. Pujolle, "Intrusion detection in 5G and Wi-Fi networks: A survey of current methods, challenges and perspectives," IEEE Access, vol. 13, pp. 40950-40976, 2025, doi: 10.1109/ACCESS.2025.3546338.

[17] K. Noor, A. L. Imoize, C.-T. Li, and C.-Y. Weng, "A review of machine learning and transfer learning strategies for intrusion detection systems in 5G and beyond," Mathematics, vol. 13, no. 7, 1088, 2025, doi: 10.3390/math13071088.

[18] K. He, D. D. Kim, and M. R. Asghar, "Adversarial machine learning for network intrusion detection systems: A comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 538-566, 2023, doi: 10.1109/COMST.2022.3233793.

[19] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems," in Proc. Military Communications and Information Systems Conference, 2015, pp. 1-6, doi: 10.1109/MilCIS.2015.7348942.

[20] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in Proc. International Conference on Information Systems Security and Privacy, 2018, pp. 108-116, doi: 10.5220/0006639801080116.

[21] Francis Onojah, Prof. Prema Kirubakaran, Dr. Ridwan Kolapo, Dr.Temitope Olufunmi Atoyebi, Dr. R. Renuga Dev. Improving DDoS Detection in Software-Defined Networks through a Hybrid Machine Learning 2025, Department of Information Technology, Nile University of Nigeria. Abuja.Nigeria Iconic Research and Engineering Journals, Volume 9, Issue 3, ISSN: 2456-8880