Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X
Volume 4, Issue 2, 2026

SMARTSHIELD: INTRUSION DETECTION SYSTEM FOR IOT TRAFFIC USING MACHINE LEARNING

Muhammad Ahmad Khan[*1], Muhammad Adil[2], Sohaib Ahmad[3], Zain Ul Abiden Akhtar[4]

[*1,2,3,4]*Department of Information & Communication Engineering,The Islamia University Bahawalpur*

[*1]akhan895471@gmail.com

DOI: https://doi.org/10.5281/zenodo.18783593

Keywords
Internet of Things, Intrusion Detection Systems, Machine Learning, Deep Learning, Network Security

Article History
Received on 19 Jan, 2026
Accepted on 20 Feb, 2026
Published on 26 Feb, 2026

Corresponding Author: Muhammad Ahmad Khan

Abstract

The IoT network has developed into a rapid proliferation making the surface of cyber-attack large because of device heterogeneity and limitation of resources. Conventional intrusion detection systems are unable to cope with volatile IoT traffic, which encourages having ML-based solutions. In this paper, the systematic review of ML-based intrusion detection of an IoT is carried out, which divides the approaches into supervised, unsupervised, deep learning, ensemble, and federated learning models. We evaluate benchmark data sets (such as NSL-KDD, BoT-IoT, CICIoT2023, IoT-23 and TON IoT) and investigate their results, such as accuracy, as well as latency, scalability, and resource consumption. Such issues as class imbalance, concept drift, adversarial evasion, and edge-device limitations are pointed out as the main deployment issues. Such emerging trends are federated learning, explainable AI, and lightweight architectures. The insights presented in this review can be structured to design effective intrusion detection systems in the next-generation IoT environment.

I. Introduction

IoT has transformed healthcare, smart cities, and industrial intelligent agriculture and unites billions of devices all over the world [1], [2]. This expansion however comes with a severe security gap [3]–[6]. The diversity and low computing power of the IoT devices pose special issues in the field of security [7], [8], DDoS attacks, botnets, and data breaches become commonplace, and the latter become systematized [9], . Fig. 1 gives the figures of IoT development and the attacks between 2018 and 2025.

ML and DL have a potential remedy to the issue of detection of IoT intrusions [11]–[14]. DDoS, man-in-the-middle, spoof- ing, and malware injections are typical attacks to consider, and resource limitations make ML-based detection an appealing option to be considered [15]–[18], which is supported by the problem of finite resources of devices, software, and so on [19], [20].

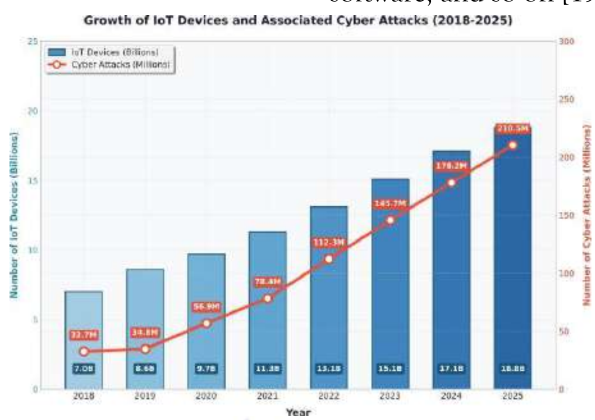


Fig. 1. Growth of IoT devices and cyber attacks (2018–2025)

This is a systematic review of ML-based IoT IDS, which makes contributions in the following ways: (1) taxonomy of schemes in ML techniques, (2) data and metric analysis, (3) challenge, (4) future directions. The comparison between existing surveys is organized in Table I [21]

Table I: Comparison Of Existing Surveys On Ml-Based Iot-Ids

Survey	Year	ML	DL	FL	XAI	Data	Chall.	Focus
Kikissagbe [1]	2024	✓	✓	×	×	✓	✓	ML overview
Rahman [2]	2025	✓	✓	×	×	✓	✓	IoT-IDS
Bilot [21]	2024	✓	✓	×	×	✓	×	GNN-based
Arnob [5]	2025	✓	✓	✓	×	✓	✓	Emerging tech
Khan [24]	2025	✓	✓	×	✓	✓	✓	XAI Industry 5.0
Mallidi [6]	2025	✓	✓	✓	×	✓	✓	Training
Ours	**2025**	✓	✓	✓	✓	✓	✓	**ML/DL/FL/XAI**

II. Fundamentals of IoT and Intrusion Detection

A. IoT Architecture and Communication Protocols

IoT architecture is divided into three layers: perception, network, and application with distinct security issues of their own [25]–[28]. This architecture with security vulnerabilities at every stage is depicted in Fig. 2.

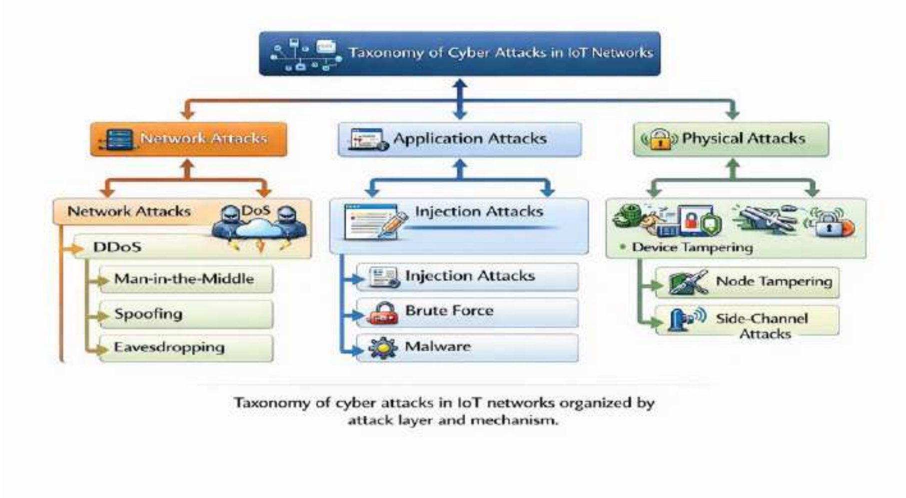


Fig. 2. Three-layer IoT architecture with security vulnerabilities.

The competitors of protocols (MQTT, CoAP, Zigbee, BLE) pose another complexity to IDS [29]–[32].

B. Threat Taxonomy for IoT Networks

IoT networks are vulnerable to different cyber threats classified in terms of target layer, mechanism, and impact [33]–[38]. In Fig. 3 is provided in detail.

Fig. 3. Classification of cyber attacks targeting IoT networks.

Attacks by botnets such as Mirai have become common where vulnerable devices are being used to carry out massive attacks in large scale attacks [39]–[41].Table II gives an attack taxonomy.

Table II: Taxonomy Of Iot Attack Types

Layer	Attack Type	Description	Examples	Impact
	DDoS	Overwhelming target with traffic	UDP/SYN flood	Service disruption
Network	MITM	Intercepting communications	ARP spoofing	Data theft
	Routing	Manipulating network routes	Sinkhole, Wormhole	Traffic diversion
	Reconnaissance	Network scanning/probing	Port scanning	Info gathering
Application	Injection	Malicious code injection	SQL injection, XSS	Unauthorized access
	Brute Force	Credential guessing	Password attacks	Account compromise
	Malware	Malicious software	Mirai, Hajime	Device compromise
Perception	Spoofing	Fake sensor data	GPS spoofing	False data injection
	Tampering	Hardware manipulation	Node capture	Device compromise

C. *IDS Classification and Deployment*

There are signature-based (high accuracy when known threat) and anomaly-based (ability to detect zero-day threats) IDS [43]–[48]. There are hybrid techniques, combining the two methods in order to provide complete coverage citeabdelaziz2025federated, ohtani2024idac, mahmud2024privacy. There are deployment strategies which are: NIDS, HIDS, and lightweight edge based mechanisms [53]–[59].

III. MACHINE LEARNING TECHNIQUES FOR IOT-IDS

Fig. 4 provides the taxonomy of ML methods used in IoT-IDS.

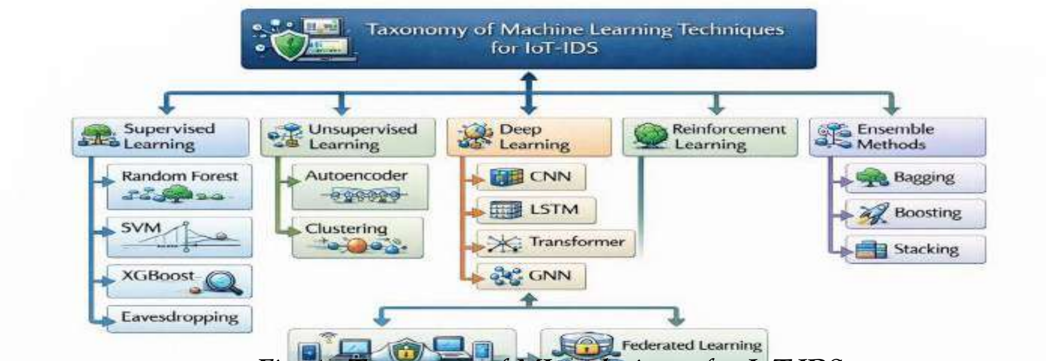


Fig. 4. Taxonomy of ML techniques for IoT-IDS.

A. *Supervised Learning*

Classification supervised algorithms such as Random Forest, SVM, and XGBoost are also used on the identified datasets with labeled data in use into classification-capable supervised algorithms used on ranked order optimization piping networks classifications or on models to detect patterns in data classification [4], [31], Random Forest has 91.7% accuracy with Top-10 features selection and processes take 35% less time with Top-10 features selected compared to Top- 10 Adversary features selected [27], With good choice of features, XGBoost performs better [30].

B. *Unsupervised and Semi-Supervised Methods*

Unsupervised learning is a type of minimum zero-data attack detection with clustering (K-means, DBSCAN, Isolation Forest) that uses unlabeled data and does not depend on labelling, unlike self-supervised data learning instruments such as basic linear models [61], [62]. Auto encoders detect anomalies through errors in reconstruction, and it is its most efficient in real-time identification of anomalies in multilayer detection [56], [60], Semi-supervised learners use a small number of labeled data and a huge amount of unlabeled data [46],

C. *Deep Learning Architectures*

Deep learning allows auto-feature extraction of IoT-IDS as algorithmic features can be calculated automatically as well as other features that cannot be measured by traditional features that are calculated manually and that cannot be measured automatically by algorithms [8], [13], [13], Common DL architectures are presented in Fig. 5.

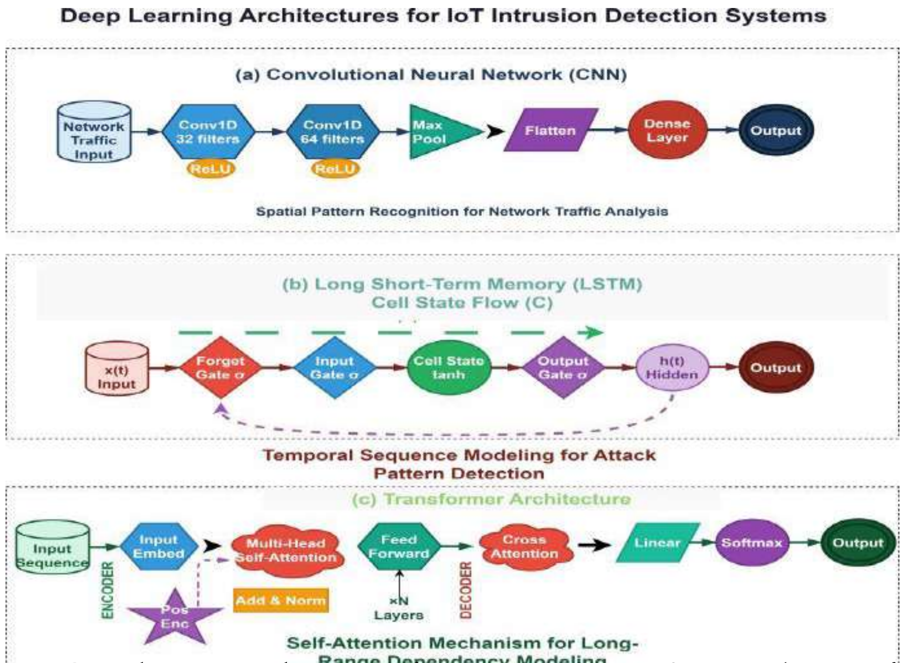


Fig. 5. Deep learning architectures for IoT-IDS: CNN, LSTM, and Trans- former.

The accuracy of hybrid CNN-LSTM is 99.87% and the FPR is 0.13% Long-range dependencies are learnt through attention mechanisms on transformers to capture them accurately and boost interactions with them at a greater distance than with current systems [26], [67]. GNNs are effective to model the network topology [37].

D. *Reinforcement and Ensemble Methods*

Benefits Adaptive IDS: RL is a method that learns optimal policy by interacting with the environment Proponents RL is an adaptive IDS, able to learn optimal policies through interaction with the environment Cited importance in practice Knowledge bases Advisory RL, like other adaptive IDS, can optimize policies by engaging with the environment. Ensemble (bagging, boosting, and stacking) methods are more accurate and robust as well as resistant to data therapy [63]–[65].

A comparative summary of ML algorithm output in the case of IoT-ID is presented in Table III.

IV. Benchmark Datasets and Evaluation Metrics

A. *Traditional and IoT-Specific Datasets*

The evaluation of IDS has been significantly conducted on traditional datasets (KDD Cup 99, NSL-KDD, UNSW-NB15) [10], [17], [47],

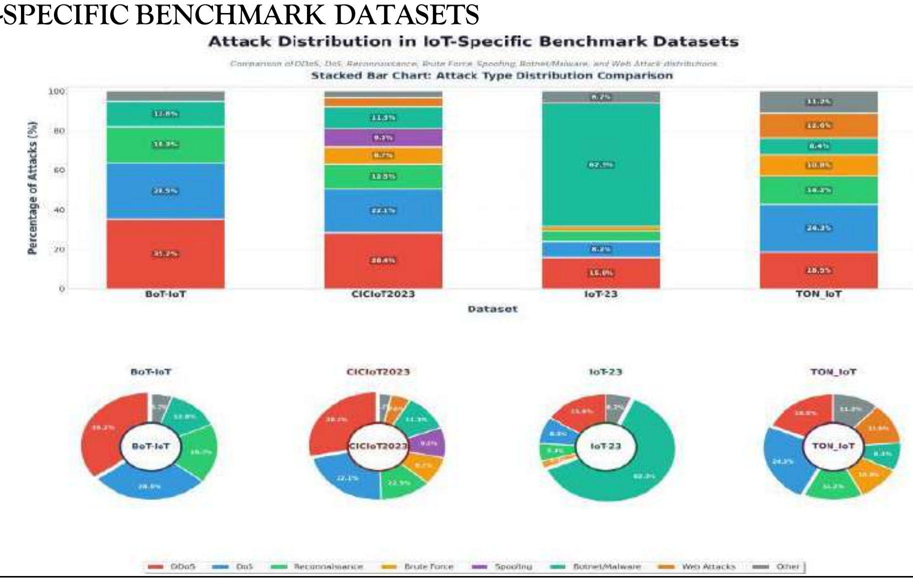
Certain datasets contain a better representation of unique traffic patterns: IoT-specific BoT-IoT includes botnet traffic [34], just in this category, [68], also industrial IoT Edge-IIoTset The attack distributions in datasets are presented in Fig. 6.

TABLE III: PERFORMANCE COMPARISON OF ML ALGORITHMS FOR IOT-IDS

Category	Algorithm	Acc.	F1	Advantages	Limitations	Refs.
Supervised	Random Forest	91–98%	0.92–0.97	High-dim, robust	Labeled data needed	[31], [32]
	XGBoost	93–99%	0.94–0.98	High accuracy	Computational cost	[10], [29]
	SVM	89–96%	0.90–0.95	Binary classification	Scalability	[3], [4]
Unsupervised	Autoencoder	95–98%	0.93–0.97	Zero-day detection	Higher FP	[20], [56]
	Isolation Forest	92–97%	0.91–0.96	Anomaly isolation	Parameter sensitive	[42], [48]
	CNN	96–99%	0.95–0.98	Spatial features	High computation	[8], [14]
Deep Learning	LSTM	97–99%	0.96–0.98	Temporal patterns	Slow training	[13], [28]
	CNN-LSTM	98–99.87%	0.97–0.99	Spatial-temporal	Complex	[27], [65]
	Transformer	96–98%	0.95–0.97	Long-range deps	Resource intensive	[26], [66]
Graph-based	GNN/GAT	94–98%	0.93–0.97	Topology modeling	Complexity	[21], [35]
Federated	FL + DL	94–99%	0.93–0.98	Privacy-preserving	Comm. overhead	[45], [54]

Fig. 6. Attack distribution in IoT-specific benchmark datasets.

TABLE IV: IOT-SPECIFIC BENCHMARK DATASETS



Dataset	Year	Samples	Feat.	Attack Types	Devices	Refs.
BoT-IoT	2019	73M+	46	DDoS, DoS, Recon, Theft	Smart home	[28], [34]
CICIoT2023	2023	47M+	46	33 attacks (7 categories)	105 IoT devices	[17], [68]
IoT-23	2020	325M+	21	Mirai, Torii, Gagfyt	IoT malware	[42], [59]
TON_IoT	2020	461K+	44	DoS, Ransomware, Injection	Industrial IoT	[9], [57]
Edge-IIoTset	2022	2M+	61	14 attack types	Edge/IIoT	[15], [25]
NSL-KDD	2009	148K	41	DoS, Probe, R2L, U2R	Traditional	[32], [41]
UNSW-NB15	2015	2.5M	49	Backdoor, Exploits, Worms	Modern network	[47],

B. Performance Metrics and Dataset Limitations

The evaluation metrics must contain accuracy, precision, recall, F1-score, and AUC-ROC and computational efficiency (training/inference time, memory) to constrained resources (objectively and sustainably) will require evaluation [12], Weaknesses of datasets are the old attacks, lack of

Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X
Volume 4, Issue 2, 2026

emerging threats, and privacy issues that restrict their practice in the real-world [5], [6], [9], [40], [54],

V. CHALLENGES AND OPEN ISSUES

A. Class Imbalance and Data Scarcity

The imbalance between classes is vast because the number of normal traffic significantly exceeds the number of attacks [58], This is dealt with by SMOTE, under sampling and cost-sensitive learning, among others, as discussed in the construction and correction of neural networks as well-being, respectively, Fig. 7 is a visualization of the issue and the methods of its management. Such lack-of-information restricts effective training; transfer learning and synthetic data generation can be solutions [39],

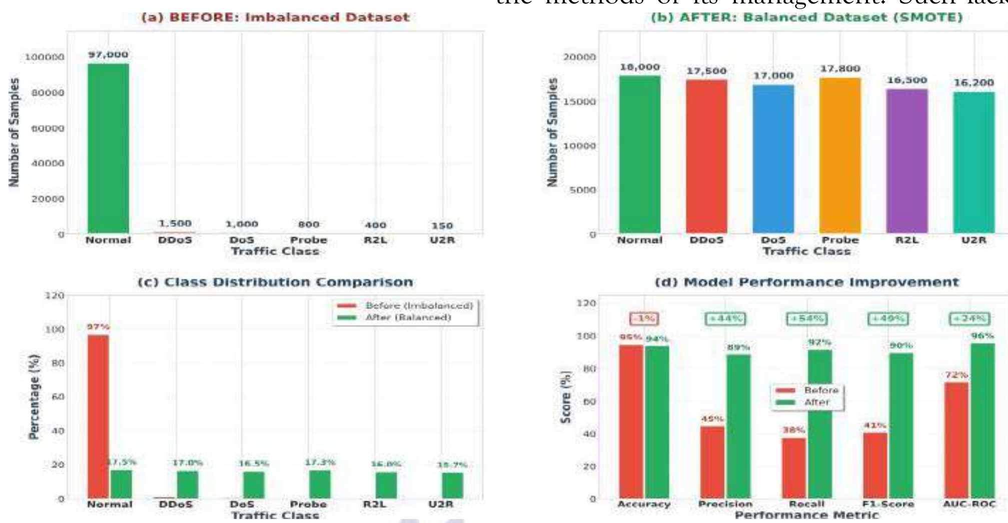


Fig. 7. Class imbalance visualization and handling techniques.

B. Real-Time Processing and Resource Constraints

IoT needs to be real-time and with low latency in detection of things There should be lightweight architectures, model compression, and edge deployment, which are fundamental roles of the model approach to apply to the choice of software development and infrastructure must be software engineering, not hardware engineering, [16], Constrained device deployment is possible through model quantization, pruning and knowledge distillation [52],

C. Adversarial Attacks and Privacy Concerns

Adversarial evasion attacks compromise ML-based IDS, including processes that elucidate actions and observations by machines, systems, and their users, and applications located in the wilderness, as well as systems that enhance their capabilities, repair existing instances, and generate novel methods to compromise resources (including knowledge ones) [24], [57].

Sharing of data is curbed due to privacy concerns; federated learning and differential privacy are solutions to this problem [46], [49]–[51],

VI. EMERGING PARADIGMS AND FUTURE DIRECTIONS

A. Federated Learning for Distributed Detection

Federated learning allows the collaborative training in which centralizing sensitive data does not occur, but rather, collaboratively [44], The framework is depicted in Fig. 8 federated learning.

Positive outcomes are demonstrated by graph-based federated techniques [53]–[55].

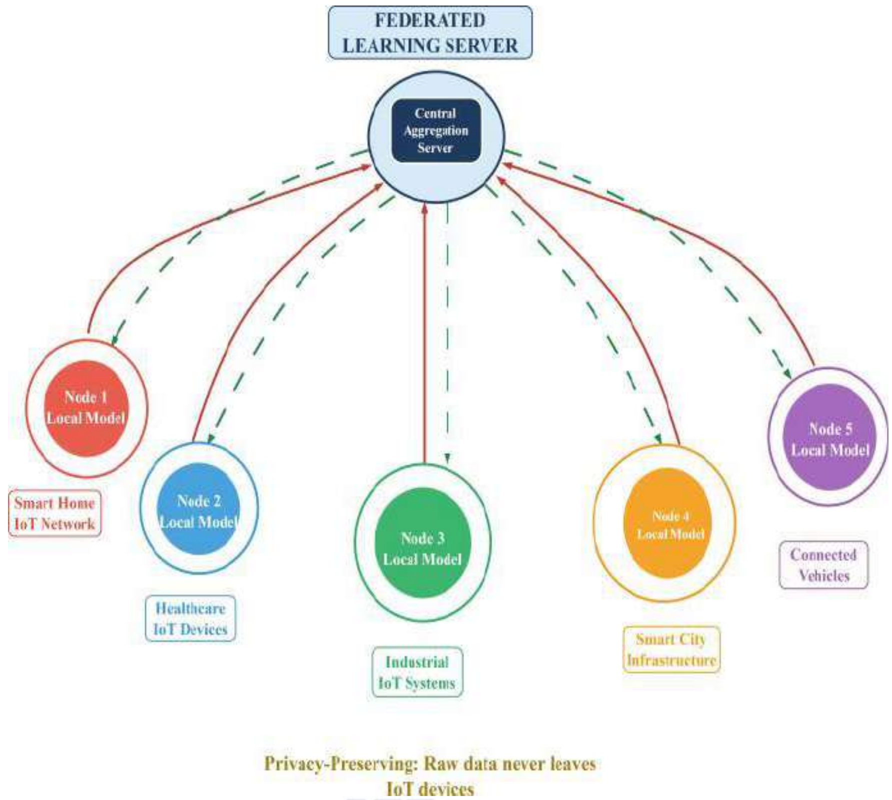


Fig. 8. Federated learning framework for privacy-preserving IoT-IDS.

B. Explainable AI and Transfer Learning

XAI allows transparent detection information based on SHAP, Lime, and attention visualization [22]–[24], Transfer learning facilitates transfer of knowledge over fields

C. SDN Integration and Quantum-Resistant Frameworks

SDN offers flexible ML-IDS deployment systems with central monitoring of traffic

[35]–[37]. The research into quantum-resistant security is stimulated by the appearance of quantum computing

VII. Comparative Analysis and Discussion

A. Performance Comparison

Slapstick-Comparison Trade-offs between accuracy, efficiency and generalization are seen between hybrid AI makers Fig. 9 shows the comparison of the performance in terms of measures.

Fig. 9. Performance comparison radar chart of ML techniques.

Ensemble methods show strong performance CNN-BiLSTM achieves highest F1 (0.986) with higher over- head Transformers show promise for complex patterns [67]. Table V provides comprehensive comparison with research gaps.

TABLE V: COMPREHENSIVE COMPARISON OF ML TECHNIQUES

Technique	Accuracy	Inference	Edge	Strength	Research Gaps
Random Forest	98.5%	Fast	Yes	Interpretability	Limited temporal modeling
XGBoost	99.1%	Fast	Yes	Feature importance	Hyper parameter sensitive
CNN	99.2%	Medium	Partial	Spatial features	Lacks temporal context
LSTM	99.5%	Slow	No	Temporal sequences	High computational cost
CNN-LSTM	99.87%	Slow	No	Spatial-temporal	Very resource intensive
Transformer	98.8%	Medium	No	Long-range deps	Large model size
GNN	98.2%	Medium	Partial	Topology awareness	Complex graph construction
Federated	99.0%	Variable	Yes	Privacy preservation	Communication overhead
Autoencoder	97.8%	Fast	Yes	Zero-day detection	Higher false positives

B. *Research Gaps and Future Directions*

Key gaps include: lightweight accurate models adversarial robustness standardized evaluation and privacy-preservation [45], Fig. 10 presents the research roadmap.

Fig. 10. Research gaps and future directions roadmap for ML-based IoT-IDS.

The next wave of research should be introduced to cohesive frameworks and multi-disciplinary interaction [6], [69]-[72], [52].

VIII. Conclusion

This review discussed the use of ML-based intrusion detection to into networks, which involves supervised, unsupervised, deep learning, ensemble, federated learning, and XAI architectures. The important issues such as the imbalance of classes, the real-time processing, the adversarial robustness, and resource must be mentioned. As IoT continues to implement both the critical infrastructures and also other important infrastructures, designing, and implementing power efficient IDS would be the most significant when it comes to the protection of the ecosystem against the emerging threats.

References

[1] B. R. Kikissagbe and M. Adda, "Machine learning-based intrusion detection methods in IoT systems: A comprehensive review," *Electronics*, vol. 13, no. 18, p. 3601, 2024.

[2] M. M. Rahman, S. A. Shakil, and M. R. Mustakim, "A survey on intrusion detection system in IoT networks," *Cyber Security and Applications*, vol. 3, p. 100082, 2025.

[3] A. Almotairi, S. Atawneh, and A. Osama, "Enhancing intrusion detection in IoT networks using machine learning-based feature selection and ensemble models," *Systems Science & Control Engineering*, vol. 12, no. 1, p. 2321381, 2024.

[4] S. Walling and S. Lodh, "Network intrusion detection system for IoT security using machine learning and statistical based hybrid feature selection," *Security and Privacy*, vol. 7, no. 4, p. e429, 2024.

[5] A. K. B. Arnob *et al.*, "A comprehensive systematic review of intrusion detection systems: emerging techniques, challenges, and future research directions," *Journal of Edge Computing*, vol. 4, no. 1, pp. 73–104, 2025.

[6] S. K. R. Mallidi and R. R. Ramisetty, "Advancements in training and deployment strategies for AI-based intrusion detection systems in IoT: A systematic literature review," *Discover Internet of Things*, vol. 5, no. 1, p. 8, 2025.

[7] M. A. Alsoufi *et al.*, "Anomaly-based intrusion detection model using deep learning for IoT networks," *Computer Modeling in Engineering & Sciences*, vol. 141, no. 1, pp. 823–845, 2024.

[8] M. Nakip and E. Gelenbe, “Online self-supervised deep learning for intrusion detection systems,” *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 5765–5779, 2024.

[9] M. Gelgi *et al.*, “Systematic literature review of IoT botnet DDoS attacks and evaluation of detection techniques,” *Sensors*, vol. 24, no. 11, p. 3571, 2024.

[10] M. Nawaz *et al.*, “Lightweight machine learning framework for efficient DDoS attack detection in IoT networks,” *Scientific Reports*, vol. 15, p. 24961, 2025.

[11] J. Li *et al.*, “Optimizing IoT intrusion detection system: Feature selection versus feature extraction in machine learning,” *Journal of Big Data*, vol. 11, no. 1, p. 36, 2024.

[12] S. Yaras and M. Dener, “IoT-based intrusion detection system using new hybrid deep learning algorithm,” *Electronics*, vol. 13, no. 6, p. 1053, 2024.

[13] D. Kilichev and D. Turimov, “Next-generation intrusion detection for IoT EVCS: Integrating CNN, LSTM, and GRU models,” *Mathematics*, vol. 12, no. 4, p. 571, 2024.

[14] J. A. Alzubi, O. A. Alzubi, and A. Singh, “A blended deep learning intru- sion detection framework for consumable edge-centric IoMT industry,” *IEEE Trans. Consumer Electronics*, vol. 70, no. 1, pp. 1256–1267, 2024.

[15] D. Rupanetti and N. Kaabouch, “Combining edge computing-assisted Internet of Things security with artificial intelligence: Applications, challenges, and opportunities,” *Applied Sciences*, vol. 14, no. 16, p. 7104, 2024.

[16] T. Zhukabayeva *et al.*, “Cybersecurity solutions for industrial Internet of Things–edge computing integration: Challenges, threats, and future directions,” *Sensors*, vol. 25, no. 1, p. 213, 2025.

[17] N. U. Ahmad *et al.*, “Securing IoT networks against DDoS attacks: A hybrid deep learning approach,” *Sensors*, vol. 25, no. 5, p. 1346, 2025.

[18] S. Malekzadeh, S. Yousefi, and M. S. Tajbakhsh, “DDoS prevention in IoT networks by analyzing source-side inter-bot traffic using deep learning techniques,” *The Journal of Supercomputing*, vol. 81, p. 742, 2025.

[19] X. Chen *et al.*, “Resource-constraint deep forest-based intrusion detec- tion method in Internet of Things for consumer electronic,” *IEEE Trans. Consumer Electronics*, vol. 70, no. 2, pp. 4976–4987, 2024.

[20] A. G. Ayad *et al.*, “Efficient real-time anomaly detection in IoT networks using one-class autoencoder and deep neural network,” *Electronics*, vol. 14, no. 1, p. 104, 2024.

[21] T. Bilot *et al.*, “Graph neural networks for intrusion detection: A survey,” *IEEE Access*, vol. 11, pp. 49114–49139, 2024.

[22] O. Arreche *et al.*, “XAI-IDS: Toward proposing an explainable artifi- cial intelligence framework for enhancing network intrusion detection systems,” *Applied Sciences*, vol. 14, no. 10, p. 4170, 2024.

[23] A. AlAbbadi and F. Bajaber, “An intrusion detection system over the IoT data streams using explainable artificial intelligence (XAI),” *Sensors*, vol. 25, no. 3, p. 847, 2025.

[24] N. Khan *et al.*, “Explainable AI-based intrusion detection systems for Industry 5.0 and adversarial XAI: A systematic review,” *Information*, vol. 16, no. 12, p. 1036, 2025.

[25] T. Zhukabayeva *et al.*, “An edge-computing-based integrated framework for network traffic analysis and intrusion detection to enhance cyber- physical system security in industrial IoT,” *Sensors*, vol. 25, no. 8, p. 2395, 2025.

[26] Z. Long *et al.*, “A transformer-based network intrusion detection approach for cloud security,” *Journal of Cloud Computing*, vol. 13, no. 1, p. 5, 2024.

[27] S. S. Bamber *et al.*, “A hybrid CNN-LSTM approach for intelligent cyber intrusion detection system,” *Computers & Security*, vol. 148, p. 104146, 2025.

[28] P. Sinha *et al.*, "A high performance hybrid LSTM CNN secure architecture for IoT environments using deep learning," *Scientific Reports*, vol. 15, no. 1, p. 9684, 2025.

[29] M. Sajid *et al.*, "Enhancing intrusion detection: a hybrid machine and deep learning approach," *Journal of Cloud Computing*, vol. 13, no. 1, p. 123, 2024.

[30] J. Liu *et al.*, "An intrusion detection system on the Internet of Things using deep learning and multi-objective enhanced gorilla troops optimizer," *Journal of Bionic Engineering*, vol. 21, no. 3, pp. 1397–1411, 2024.

[31] K. B. Médard *et al.*, "Top-K feature selection for IoT intrusion detection: Contributions of XGBoost, LightGBM, and Random Forest," *Future Internet*, vol. 17, no. 11, p. 529, 2025.

[32] V. R. Joshi *et al.*, "Hybrid AI intrusion detection: Balancing accuracy and efficiency," *Sensors*, vol. 25, no. 24, p. 7564, 2025.

[33] B. Susilo, A. Muis, and R. F. Sari, "Intelligent intrusion detection system against various attacks based on a hybrid deep learning algorithm," *Sensors*, vol. 25, no. 2, p. 580, 2025.

[34] A. S. Ahanger *et al.*, "Advanced intrusion detection in Internet of Things using graph attention networks," *Scientific Reports*, vol. 15, no. 1, p. 9831, 2025.

[35] J. Zhang, X. Fan, and Z. Zhao, "A hybrid intrusion detection model based on dynamic spatial-temporal graph neural network in in-vehicle networks," *Scientific Reports*, vol. 15, no. 1, p. 34736, 2025.

[36] H.-D. Le and M. Park, "Enhancing multi-class attack detection in graph neural network through feature rearrangement," *Electronics*, vol. 13, no. 12, p. 2404, 2024.

[37] B. Hua and H. Xi, "A privacy preserving intrusion detection framework for IIoT in 6G networks using homomorphic encryption and graph neural networks," *Scientific Reports*, vol. 15, p. 32087, 2025.

[38] C. Mahjoub *et al.*, "An adversarial environment reinforcement learning- driven intrusion detection algorithm for Internet of Things," *EURASIP J. Wireless Commun. Netw.*, vol. 2024, no. 1, p. 21, 2024.

[39] S. Balaji *et al.*, "A GAN-based hybrid deep learning approach for enhancing intrusion detection in IoT networks," *Int. J. Adv. Comput. Sci. Appl.*, vol. 15, no. 6, p. 637, 2024.

[40] A. Bennour *et al.*, "An innovative framework to securely transfer data through the Internet of Things using advanced generative adversarial networks," *Int. J. Distrib. Sensor Netw.*, vol. 21, no. 1, pp. 1–15, 2025.

[41] Y. Chen, X. Zheng, and N. Wang, "Construction of VAE-GRU-XGBoost intrusion detection model for network security," *PLoS ONE*, vol. 20, no. 6, p. e0326205, 2025.

[42] S. Üstebay, "Improving zero-day attack detection accuracy in IoT networks with isolation forest and tree-based models," *Electrica*, vol. 25, p. 0177, 2025.

[43] J. A. Shaikh *et al.*, "A deep reinforcement learning-based robust intrusion detection system for securing IoMT healthcare networks," *Frontiers in Medicine*, vol. 12, p. 1524286, 2025.

[44] J. Xie, "Application study on the reinforcement learning strategies in the network awareness risk perception and prevention," *Int. J. Comput. Intell. Syst.*, vol. 17, no. 1, p. 112, 2024.

[45] A. Karunamurthy *et al.*, "An optimal federated learning-based intrusion detection for IoT environment," *Scientific Reports*, vol. 15, p. 8696, 2025.

[46] B. Olanrewaju-George and B. Pranggono, "Federated learning-based intrusion detection system for the Internet of Things using unsupervised and supervised deep learning models," *Cyber Security and Applications*, vol. 3, p. 100068, 2025.

[47] Z. Dai *et al.*, "An intrusion detection model to detect zero-day attacks in unseen data using machine learning," *PLoS ONE*, vol. 19, no. 9, p. e0308469, 2024.

[48] Y. Guo and X. Xiang, "Emerging AI threats in cybercrime: a review of zero-day attacks via machine, deep, and federated learning," *Knowledge and Information Systems*, vol. 67, pp. 1–45, 2025.

[49] M. Abd Elaziz *et al.*, "Federated learning framework for IoT intrusion detection using tab transformer and nature-inspired hyperparameter optimization," *Frontiers in Big Data*, vol. 8, p. 1526480, 2025.

[50] T. Ohtani, R. Yamamoto, and S. Ohzahata, "IDAC: Federated learning- based intrusion detection using autonomously extracted anomalies in IoT," *Sensors*, vol. 24, no. 10, p. 3218, 2024.

[51] S. A. Mahmud *et al.*, "Privacy-preserving federated learning-based intrusion detection technique for cyber-physical systems," *Mathematics*, vol. 12, no. 20, p. 3194, 2024.

[52] H. Peng *et al.*, "FD-IDS: Federated learning with knowledge distillation for intrusion detection in non-IID IoT environments," *Sensors*, vol. 25, no. 14, p. 4309, 2025.

[53] F. Mohammadzadeh *et al.*, "Privacy-preserving federated learning-based intrusion detection system for IoHT devices," *Electronics*, vol. 14, no. 1,
p. 67, 2025.

[54] F. Al Tfaily *et al.*, "Graph-based federated learning approach for intrusion detection in IoT networks," *Scientific Reports*, vol. 15, no. 1,
p. 41264, 2025.

[55] S. E. Sorour *et al.*, "LSTM-JSO framework for privacy preserving adaptive intrusion detection in federated IoT networks," *Scientific Reports*, vol. 15, no. 1, p. 11321, 2025.

[56] K. Saranya and A. Valarmathi, "A multilayer deep autoencoder approach for cross layer IoT attack detection using deep learning algorithms," *Scientific Reports*, vol. 15, p. 10246, 2025.

[57] V. Morshedi *et al.*, "A comprehensive review of deep learning techniques for anomaly detection in IoT networks: Methods, challenges, and datasets," *Engineering Reports*, vol. 7, no. 10, p. e70415, 2025.

[58] R. Al-Qurashi *et al.*, "Intelligent intrusion detection system against various attacks based on a hybrid deep learning algorithm," *Sensors*, vol. 25, no. 2, p. 580, 2025.

[59] Y. Wang *et al.*, "A review of deep learning applications in intrusion detection systems: Overcoming challenges in spatiotemporal feature extraction and data imbalance," *Applied Sciences*, vol. 15, no. 3, p. 1552, 2025.

[60] M. M. Aslam *et al.*, "An improved autoencoder-based approach for anomaly detection in industrial control systems," *Systems Science & Control Engineering*, vol. 12, no. 1, p. 2334303, 2024.

[61] Y. Xiao, Y. Feng, and K. Sakurai, "An efficient detection mechanism of network intrusions in IoT environments using autoencoder and data partitioning," *Computers*, vol. 13, no. 10, p. 269, 2024.

[62] H. Rhachi, Y. Balboul, and A. Bouayad, "Enhanced anomaly detection in IoT networks using deep autoencoders with feature selection tech- niques," *Sensors*, vol. 25, no. 10, p. 3150, 2025.

[63] Y. K. Saheed, O. H. Abdulganiyu, and T. A. Tchakoucht, "Modified genetic algorithm and fine-tuned long short-term memory network for intrusion detection in the Internet of Things networks with edge capabilities," *Applied Soft Computing*, vol. 155, p. 111434, 2024.

[64] V. Saravanan *et al.*, "IoT-based blockchain intrusion detection using optimized recurrent neural network," *Multimedia Tools and Applications*, vol. 83, no. 11, pp. 31505–31526, 2024.

[65] D. M. A. A. Afraji, J. Lloret, and L. Peñalver, "An integrated hybrid deep learning framework for intrusion detection in IoT and IIoT networks using CNN-LSTM-GRU architecture," *Computation*, vol. 13, no. 9,
p. 222, 2025.

[66] A. Almadhor *et al.*, "Evaluating large transformer models for anomaly detection of resource-constrained

IoT devices for intrusion detection system," *Scientific Reports*, vol. 15, no. 1, p. 37972, 2025.

[67] X. Liu *et al.*, "Research on intrusion detection method based on transformer and CNN-BiLSTM in Internet of Things," *Sensors*, vol. 25, no. 9, p. 2725, 2025.

[68] A. Ikhlaq, A. Abbass, M. A. Khan, A. Ullah, and Z. ul Abiden, "Semantics over syntax: A deep Bi-LSTM framework for robust password strength estimation via hybrid ground-truth labeling," *Spectrum of Engineering Sciences*, vol. 4, no. 2, pp. 547–561, 2026.

[69] Z. A. Shahid, S. Amin, A. Sufyan, and A. Majeed, "Aerostrike: A real-time AI-driven framework for wireless network threat detection and exploitation," *Spectrum of Engineering Sciences*, vol. 4, no. 1, pp. 697–710, 2026.

[70] A. Sufyan, M. Mujeeb-Ur-Rehman, B. Noreen, and S. Amin, "Trends, capabilities, and challenges in modern cyber defense: A systematic review of detection and response technologies," *Spectrum of Engineering Sciences*, vol. 4, no. 1, pp. 464–503, 2026.

[71] A. M. Alashjaee and F. Alqahtani, "Enhanced intrusion detection system IoT network security model by feed forward neural network and machine learning," *Scientific Reports*, vol. 15, p. 36085, 2025.

[72] Ullah, Atta & Ahmed, Faheem & Tariq, Sana & Haider, Iram. (2025). Breaking Secure CAPTCHA using Deep Learning.