International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(10s) 2026 pp. 1056-1065
https://doi.org/10.70917/ijcisim-2026-3696
Article

# Artificial Intelligence-Based Intrusion Detection Systems for Cloud and Internet of Things (IoT) Environments

**A. Arul Anitha[1], Anand R[2], Arpita Nath Boruah[3], Arun Raj S.R.[4]**

[1]Department of Computer Applications, Jayaraj Annapackiam College for Women (Autonomous), Periyakulam, Theni Dt., Tamil Nadu, India.
Email: arulanita@gmail.com
[2]Department of Computer Science and Engineering, Easwari Engineering College, Ramapurem, Chennai.
Email: nowhereanand@yahoo.com
[3] Faculty of Computer Technology, Assam Down Town University, Shankar Madhab Path, Gandhi Nagar, Panikhaiti, Guwahati, Assam, India. Pin 781026.
Email: arpita.b@adtu.in
[4]Department of Electronics and Communication Engineering, University B.D.T College of Engineering, Davanagere-577004, Karnataka.
Email: arunrajsr5@gmail.com
ORCID: 0009-0005-7604-2658

**Abstract:** The exponentially increasing number of IoT devices and their corresponding cloud infrastructures increases the attack surface. Classic rule-based schemes and cryptographic solutions are not well adapted to dynamic, heterogeneous, distributed, and resource-constrained IoT-cloud infrastructures. Artificial intelligence (AI) based techniques such as machine learning (ML), deep learning (DL) and federated learning (FL), considered as a new model for intrusion detection systems (IDS) to assess the threats in real time and respond to the threats effectively in the dynamic environment. This paper thoroughly reviews the state-of-the-art AI-based IDS in a layer-wise manner which consists of IoT and cloud stacks. It categorizes popular cyber-attacks associated with each layer (perception, network, transport, processing and application) and correlate the attacks to machine learning classifiers (SVM, KNN, Random Forest, CNN, RNN/LSTM, Autoencoder) at shallow and deep learning levels. The research incorporates federated IDS, graph neural networks, transformer architecture and explainable artificial intelligence as models of machine learning and further discusses prominent research issues (data scarcity, adversarial robustness, latency, transferability) and the future direction of next-generation IoT-cloud security.

**Keywords:** Intrusion detection systems, IoT security, cloud security, deep learning, machine learning, federated learning, adversarial attacks, anomaly detection, network security.

## 1. INTRODUCTION

The convergence of the Internet of Things (IoT), a global network of heterogeneous interconnected billions of smart devices, and cloud computing, the dominant computational model for scaling data processing and service delivery to a large volume of end-users, forms a large attack surface increasingly targeted by advanced adversaries [1], [2].

Traditional security methods (signature-based IDS, standard cryptography, perimeter firewall) are based on reactive architectures, and are intended for fairly homogeneous, mostly-static networks. However, these methods are not applicable to an IoT-cloud system, due to the extreme levels of device heterogeneity, limited computing resources,

and high data rates involved. A typical IoT microcontroller with a few kilobytes of RAM, for example, cannot run AES/RSA-level cryptography at the rate necessary to perform real-time traffic analysis, let alone a full IDS agent [3].

Today, AI-powered systems, especially ML and DL approaches, are considered next-generation intrusion detection technologies. Rather than relying on rules, these systems learn from past traffic to detect attacks. Compared to ML, DL-based methods are more powerful in that they can automatically learn hierarchical features from raw traffic packets without any prior feature engineering. FL can additionally address the challenges of privacy and centralized sensitive traffic data by training collaborative models distributed across multiple edge nodes [9].

Most existing surveys followed the approach of keeping IoT (or cloud) security and AI (or ML) security separate, or just provided an overview of AI/ML literature without a structured taxonomy based on the attack layer [4], [5], [7]. This paper presents a systematic, critical, and condensed survey of AI-based IDS in an integrated IoT-cloud environment. The contribution of this paper can be summarized as: (i) a layer-wise analysis of the IoT-cloud stack, mapping protocols, requirements and attack vectors, (ii) a taxonomy of AI-powered IDS (rule-based, shallow ML, deep learning and other models), (iii) tables comparing threats and countermeasures, with numerical results, and (iv) an exploration of open challenges and future research directions.

More specialized devices, such as consumer smart-home devices, industrial control systems, connected healthcare, and connected vehicles, are also proliferating, with tens of billions of such devices in existence today. These devices are always generating telemetry data, which must be constantly analyzed for signs of a security compromise. The deployment of these devices often at little or no security, with default or hard-coded passwords, and little or no firmware upgradability, leads to their often co-opted use for botnets and as launching platforms for attacks on downstream cloud infrastructure. Thus, not only does intrusion detection need to be cross-layer from the perception, network, transport, processing and application layer of the IoT-cloud stack, it needs to be supported by AI as the smart regime that unifies the diverse aspects of this heterogeneous technological ecosystem.

Section II gives an overview of the related survey works and Section III discusses the IoT-cloud architectural model. Section IV discusses security threats per layer, and Section V presents AI-based countermeasures. Section VI presents a survey of benchmark datasets. Section VII elaborates on alternative models of IDS. Section VIII discusses open challenges and future works. Section IX summarizes the paper.

## 2. RELATED SURVEY WORKS

Although there are several reviews on network intrusion detection systems and IoT security, literature on the application of AI technologies for IDSs in IoT-cloud integrated environments is limited. Previous surveys of IDSs, such as Liao et al. [1], either predate the IoT era or predate the rapid development of deep learning technologies. Mishra et al. [2] compared different ML techniques including SVM, k-NN, random forest, and ensemble classifiers for cloud-based IDS but did not cover the IoT layer. Hussain et al. [3] provided a generic overview of ML techniques for IoT security in resource-constrained environments, but did not provide a systematic review of the cloud layer or federated learning.

Al-Garadi et al. [5] presented a survey of ML and DL for IoT security along with a comparative study. They did not systematically discuss the cloud processing layer, nor the application layer threats. Tahsien et al. [7] reviewed ML-based IoT security solutions but only focused on shallow ML techniques based on a layered structure. Aldweesh et al. [6] reviewed DL-based anomaly-based IDS, but only in generic network anomaly detection, not targeted at the IoT-cloud environment. Chaabouni et al. [8] provided a survey on IoT IDS, including ML and encryption-based ones. The closest work to a layer-wise survey of IoT risks mapped to AI countermeasures is Zaman et al. [4], but it did not cover cloud-related threats, federated learning and explainability.

More comprehensively, this survey covers IoT and cloud considerations in all five layers of the architecture, including rule-based, shallow ML, DL, federated, and explainable models. We also quantitatively map known threats to countermeasures. Table 1 presents a summary and comparison.

| Reference | Year | Scope | AI/ML Coverage | IoT-Cloud Focus |
|---|---|---|---|---|
| Liao et al. [1] | 2013 | Network IDS | Rule-based, SVM | No |
| Mishra et al. [2] | 2019 | Cloud IDS | Shallow ML | Partial |

| | | | | |
|---|---|---|---|---|
| Hussain et al. [3] | 2020 | IoT security | ML and DL survey | IoT only |
| Al-Garadi et al. [5] | 2020 | IoT threats | ML/DL methods | IoT only |
| Tahsien et al. [7] | 2020 | IoT layers | Shallow ML | IoT only |
| Aldweesh et al. [6] | 2020 | Anomaly IDS | Deep learning | No |
| Chaabouni et al. [8] | 2019 | IoT IDS | ML + encryption | IoT only |
| Zaman et al. [4] | 2021 | Layer-wise IoT threats | Rule-based + shallow + DL | IoT only |
| This survey | 2026 | IoT-cloud, all layers | Rule-based, shallow, DL, FL, GNN, XAI | Full |

**TABLE 1. Comparative analysis of existing survey works.**

## 3. IOT-CLOUD ARCHITECTURAL MODEL AND SECURITY CHALLENGES

### *A. IoT-Cloud Architectural Model*

This extends from localized resources like sensors and physical computing devices, to remote cloud data centers distributed around the world. There are typically five layers, each with its own stack of protocols and security. Figure 1 below provides an illustration of this layered architecture and the placement of AI-based security.

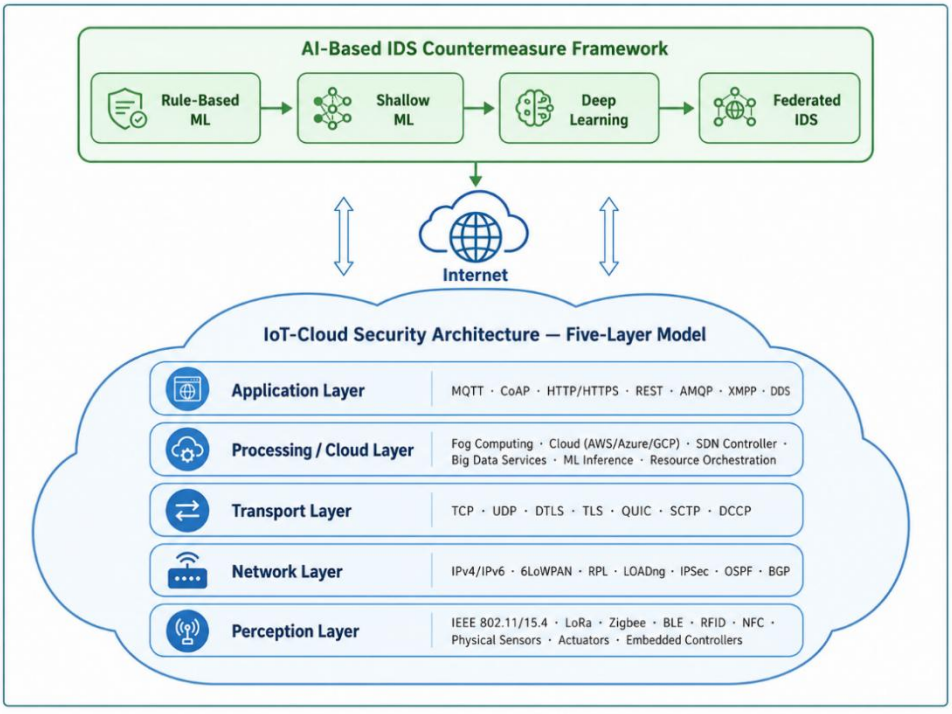


**FIGURE 1. Layered IoT-cloud security architecture illustrating protocol ecosystems and AI-based IDS placement.**

The Perception Layer is composed of heterogeneous sensor nodes, actuators and embedded controllers equipped with Wi-Fi, IEEE 802.15.4, Bluetooth Low Energy, LoRa, Zigbee, Near-Field Communication and Radio-

frequency identification. These devices are resource-constrained, physically exposed and vulnerable to physical compromise and signal-level attacks [3], [4].

The Network Layer forwards the perception layer data to a gateway, a fog node or the cloud using IPv4/IPv6, 6LoWPAN, RPL, IPSec, OSPF and BGP. Heterogeneity and low-power lossy networks complicate policy management. DDoS and routing attacks are common [4], [5].

end-to-end transport layer protocols TCP, UDP, DTLS, QUIC and SCTP are used for communication between applications. This layer may be targeted by flooding, hijacking sessions and unauthorized access [4].

The Processing/Cloud Layer consists of fog nodes, SDN controllers, and cloud services, where various operations such as data analysis, ML inference, and orchestration are performed. It provides a larger attack surface for code injection, evading ML-based defense mechanisms, and cloud-targeted VM escape attacks [2].

Application Layer services include MQTT, CoAP, HTTP/HTTPS, REST, AMQP. Vulnerabilities include phishing, browser-based attacks (e.g., cross-site scripting, tunneling) and specific MQTT attacks such as attempts through malicious code [4].

### *B. Security Challenges in IoT-Cloud Environments*

In contrast, security in the IoT-cloud ecosystem must deal with resource heterogeneity and constraints (in IoT devices such as sub-milliwatt microcontrollers to cloud servers), the dynamic and often unpredictable nature of the topology, the massive and high-velocity heterogeneous flows of data and real-time analytics, the intrinsic contradiction between protecting user privacy and training detection models on sensitive traffic, and the absence of benchmark datasets that span the whole potential IoT-cloud stack. These challenges motivate the need for adaptive, distributed, and explainable AI-based IDS architectures for the IoT-cloud ecosystem, which is the focus of the rest of this survey.

## 4. LAYER-WISE SECURITY THREAT ANALYSIS

### *A. Perception Layer Threats*

The perception layer has typical security issues attributed to physical node access, jamming and attacks leveraging the wireless medium, including jamming and spoofing, sleep-denial attacks, fake-node injection attacks and data tampering. Additional threats include jamming (injecting noise into a wireless link), spoofing (sending fake identities), sleep denial (preventing a node from entering low-power sleep mode), fake node (inserting a node into the topology of a network to capture traffic), and data tampering (injecting false or misleading sensor readings into the data stream). Jamming and sleep denial are particularly serious for implantable medical devices.

### *B. Network Layer Threats*

The network layer has been studied the most in IoT-cloud security. DDoS attacks and DoS attacks are the most destructive and most observed attacks. Doshi et al. [10] constructed a real-time IoT DDoS dataset in a home network testbed and evaluated KNN, Linear SVM, Decision Tree, Random Forest, and neural network classifiers, achieving detection rates of 91% to 99%. Routing attacks include wormhole attack, sinkhole attack, rank attack, and hello flood attack, targeting the RPL routing protocol in including 6LoWPAN ubiquitous IoT networks. Man-in-the-Middle attacks are another kind, in which attackers may eavesdrop or tamper in communication between legitimate parties, especially when devices communicate over unencrypted channels.

### *C. Transport Layer Threats*

Transport-layer or denial-of-service exploits abuse connection establishment, flow control, and data transmission processes (e.g., SYN, UDP, ACK or DNS floods) for connection denial or state table exhaustion by choking device resources. For IoT-cloud infrastructures, botnets like Mirai and its variants can construct a billion-device botnet, on a global scale, motivating federated detection with privacy considerations [9].

### *D. Processing and Cloud Layer Threats*

Attacks on the virtualized infrastructure and ML-based analytics pipelines in AI-based defense, such as fog-based attacks that hijack fog nodes as intermediaries, code injection and VM escape, and evasion attacks against ML-based detectors in which adversarial inputs are created to fool classifiers into misclassifying them as legitimate traffic while remaining semantically the same, represent important challenges.

### *E. Application Layer Threats*

The application layer is mainly focused on the protocols, APIs, and interfaces that the IoT devices use to communicate with cloud and third-party applications. Given the prevalence of MQTT protocol in IoT, it has been a target of attacks. Alaiz-Moreton et al. [12] assessed multiclass classification with GRU-RNN, XGBoost and LSTM-RNN for MQTT attack detection. They found ensemble and recurrent methods give strong, efficient performance on GPUs. SQL injection and web-based injection attacks remain a common threat of unauthorized database and application logic access.

Across all five layers, protocol aware feature sets of low computational cost are generally better suited to attacks targeting the application protocol stack (RPL routing attacks, MQTT flooding). Conversely, data-driven deep learning approaches that learn traffic behavior from raw or minimally processed flow data perform better with attacks that target aggregate statistical properties (DDoS, botnet command control). This drives the layer-wise layout of the AI-based countermeasures discussed in Section V (and further substantiates the point that no one algorithmic family is better suited to the entire IoT-cloud attack surface).

## 5. AI-BASED INTRUSION DETECTION: METHODS AND COUNTERMEASURES

### *A. Taxonomy of AI-Based IDS Approaches*

A taxonomy of AI-based IDSs for IoT-cloud environments is depicted in Figure 2. It is built on rule-based machine learning (ML) based on protocol specification or linguistics like fuzzy logic, shallow ML that include established statistical learning methods like support vector machines (SVMs), K- nearest neighbors (KNN), Random Forest, Naïve Bayes, with a manual feature engineering process, and deep learning models such as CNN, recurrent neural networks (RNN), long short term memories (LSTM), gated recurrent unit (GRU), DNN, and Autoencoder that learn in hierarchical ways. Finally, a fourth tier includes federated, graph-based, and explainable methods that aim to address the limitations of the first three tiers.

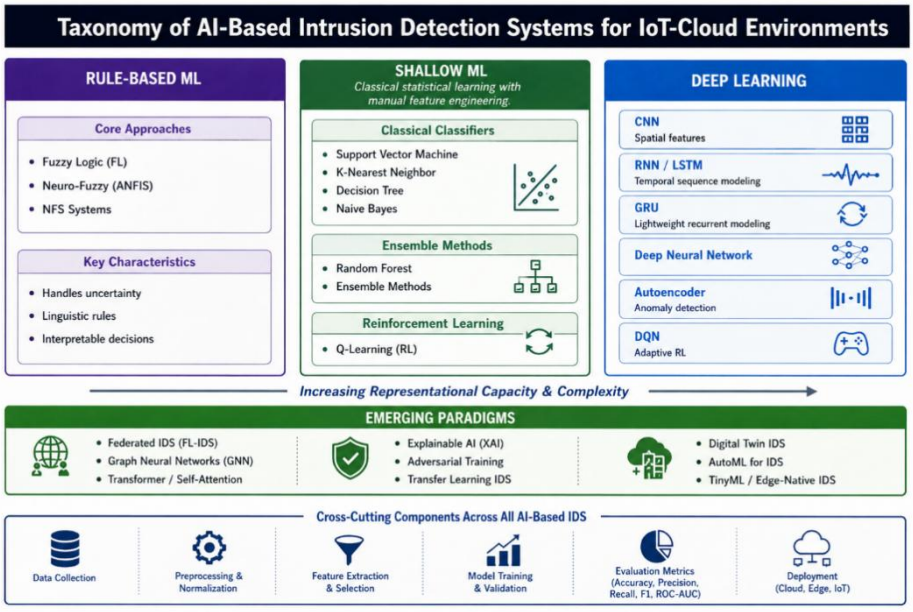


**FIGURE 2. Taxonomy of AI-based IDS techniques for IoT-cloud environments.**

### *B. Representative Layer-Wise Countermeasures*

Table 2 lists the representative AI-based countermeasures that were examined against the threats in the IoT-cloud stack and outperformed other alternatives in our surveyed studies.

| Layer / Threat | ML Type | Algorithm | Dataset | Accuracy | Ref. |
|---|---|---|---|---|---|
| Network: DoS/DDoS | Shallow ML | KNN, Linear SVM, DT, RF, NN | Real-time home network | 91–99% | [10] |
| Network: Botnet (Mirai/BASHLITE) | Deep Learning | Deep Autoencoder (N-BaIoT) | 9 real IoT devices | High detection rate | [11] |
| Application: MQTT attacks | Deep Learning | GRU-RNN, XGBoost, LSTM-RNN | MQTT-IoT dataset | GPU-efficient, high F1 | [12] |
| Network: DDoS/Recon/Theft | Shallow ML | Ensemble statistical flow features | BoT-IoT | High accuracy | [13] |
| General network intrusion | Deep Learning | DNN (multi-layer) | NSL-KDD, KDDCup99 | High accuracy | [14] |
| Transport: Malware (Mirai) | Federated Learning | DIoT self-learning anomaly detection | Distributed edge gateways | 95.6% | [9] |

**TABLE 2. Representative AI-based countermeasures across IoT-cloud layers.**

A meaningful amount of research has been conducted, about DDoS detection at the network layer. A real-time evaluation of a testbed by Doshi et al. [10], showed that even weak shallow classifiers can achieve 91%-99% accuracy by training against realistic IoT traffic. The autoencoder-based N-BaIoT approach of Meidan et al. [11] is a principled unsupervised approach and shows that reconstruction-error based anomaly detectors are effective for the detection of botnet traffic without labeled attacks. The multiclass MQTT classification of Alaiz-Moreton et al. [12] shows the generalization of recurrent and ensemble architectures to protocol-specific attacks on GPU-accelerated training. The ensemble statistical-flow-feature-based IDS of Moustafa et al. [13] and the generalized DNN-based IDS of Vinayakumar et al. [14] show that both handcrafted and end-to-end learned features perform comparably on classical benchmark datasets and IoT datasets, as validated by Ferrag et al.'s [15] comparative study of several Deep Learning architectures and datasets.

### *C. Comparative Discussion*

Taken together, the above observations (and summarized in Table 2) suggest a weak trade-off between model complexity, detection performance and deployability. Shallow ML classifiers like those investigated by Doshi et al. [10] are easily and cheaply deployable on gateway- or fog-level hardware due to their low computational resource and interpretability requirements, but are generally less successful as compared to their deep learning counterparts for more complex and novel attack variants. Deep learning based solutions (e.g. Meidan et al. [11], Vinayakumar et al. [14]) can achieve better generalization across heterogeneous traffic patterns. However, they typically need larger training datasets, more computational power, and lack of explanatory features. Federated solutions like the DIoT architecture of Nguyen et al. [9] offer a compromise of deep learning-based models with privacy preservation properties, but at the cost of additional communication and synchronization overhead on the participating nodes. The take-home message is that it is the existence of this trade-off space, rather than any specific approach to AI-IDS, that should guide practitioners.

## 6. BENCHMARK DATASETS FOR IOT-CLOUD IDS EVALUATION

The datasets used for benchmarking often greatly affect the reliability of researchers' findings in AI-based IDS. An overview of the most important datasets for testing IDS in IoT and cloud environments can be found in Table 3.

| Dataset | Year | Type | Attacks Covered | Availability |
|---|---|---|---|---|
| NSL-KDD | 2009 | Network intrusion | DoS, Probe, R2L, U2R | Public |
| CICIDS 2017 | 2017 | Network traffic | Brute force, DoS, DDoS, Botnet, Web | Public |
| BoT-IoT [13] | 2019 | IoT traffic | DDoS, DoS, Recon, Theft | Public |
| N-BaIoT [11] | 2018 | IoT botnet | Mirai, BASHLITE variants | Public |
| MQTT-IoT-IDS2020 | 2020 | MQTT protocol | DoS, Brute Force, Flooding | Public |
| Edge-IIoTset | 2022 | IIoT edge traffic | 11 attack categories incl. MITM | Public |

**TABLE 3. Benchmark datasets for IoT-cloud intrusion detection evaluation.**

Additionally, legacy datasets such as NSL-KDD suffer from statistical artifacts and do not capture the traffic diversity found in IoT systems. Compared to CICIDS 2017, though its intrusions are more realistic and diverse, it was conducted in a controlled testbed and may not sufficiently capture the heterogeneity of real-world IoT systems. BoT-IoT [13] and N-BaIoT [11] datasets from Moustafa et al. and Meidan et al. correspond to a range of IoT attacks, like flows generated from infected devices. There remain several issues: most datasets only contain edge/IoT or cloud samples, adversarial and poisoned samples are largely absent, and zero-day attacks, due to their nature, cannot be represented within the labeled datasets.

## 7. EMERGING PARADIGMS IN AI-BASED IOT-CLOUD IDS

### *A. Federated Learning for Privacy-Preserving IDS*

Federated Learning is a decentralized approach for IDS model training. It does not require the storage of traffic data in a central server. The model at each edge node is trained on data collected locally. Only model parameters or gradients are shared with the central aggregator for creating a global model update [9]. The federated IDS architecture is shown in Figure 3.

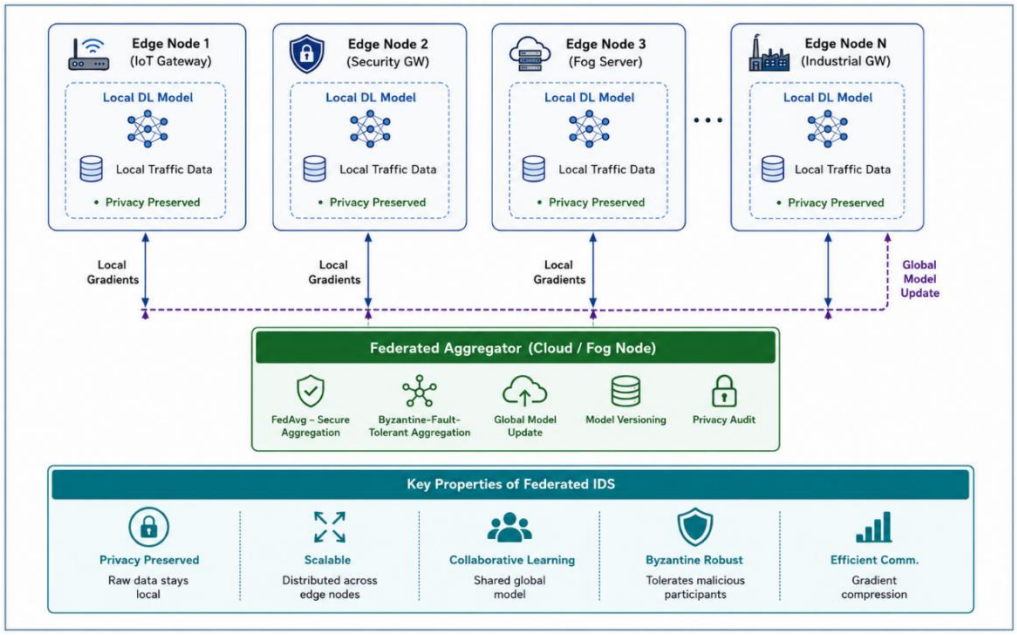


**FIGURE 3. Federated IDS architecture for distributed IoT-cloud security.**

Nguyen et al. [9] developed the DIoT system, which is the first federated IDS system in IoTs. It has a 95.6% malware detection accuracy and guarantees data locality at edge gateways. Key open challenges in federated IDS include Byzantine-fault tolerance to avoid poisoning gradient updates from participants, low communication overhead considering heterogeneous communication quality, and statistical heterogeneity between local data distributions among participants.

### *B. Graph Neural Networks and Transformer-Based IDS*

GNNs can model network traffic. Nodes represent devices or processes, and edges likely represent flows, where edges can be used for intrusion detection by modeling high-level patterns, like botnet command-and-control fan-out or lateral movement in advanced persistent threats, in the graph. These patterns can be detected using GNNs as they are not identifiable through flow-based methods. Transformer models, which use self-attention to model long-range dependencies, have also begun to be applied to network traffic because they can model the slow, distributed reconnaissance phases that exceed the context window of LSTM and GRU models.

### *C. Explainable AI and Digital Twins*

Explainability and low false positive rates of the DL-based IDSs deployed in critical infrastructure are important. XAI methods, like SHAP and LIME, provide post-hoc explanations for black-box DL models. This allows analysts to gain perception on which features of the traffic caused the detection, thereby building trust in whether the model's decision was correct. Digital twins, which are real time, high fidelity virtual models of physical systems, can be used as a complementary approach to proactive threat detection, where attacks can be simulated and synthetic training data generated while the real systems remain operational.

These techniques are often not mutually exclusive, meaning that hybrid implementations of different techniques are increasingly used in a single pipeline. For example, a federated learning architecture may be augmented with an explainability model, allowing each federated node to audit how much its traffic features contribute to the learned global model. The network topology of an IoT-cloud may also be captured by the graph in the transformer-based sequence to jointly capture the structural and temporal information of the attack, suggesting that the hybrid architecture may be the next trend of AI-based IDS for IoT-cloud environments.

## 8. OPEN CHALLENGES AND FUTURE RESEARCH DIRECTIONS

Despite meaningful progress, the task of developing effective, scalable, and trustworthy AI-based IDS for IoT-cloud environments remains an open problem. The challenges and research avenues are summarized in Table 4, and they are the main open problems in this domain.

| Challenge | Description | Potential Research Direction |
|---|---|---|
| Data Scarcity | Lack of labeled IoT-cloud attack datasets | Synthetic data generation; federated data aggregation |
| Adversarial Robustness | ML models vulnerable to evasion and poisoning | Adversarial training; certified defenses |
| Real-Time Latency | DL models too slow for real-time IoT deployment | Lightweight architectures; edge inference |
| Resource Constraints | IoT nodes have limited CPU, memory, battery | TinyML; edge-cloud split inference |
| Model Transferability | Lab-trained models fail in real deployments | Transfer learning; domain adaptation |
| Explainability | Black-box DL unacceptable in critical infrastructure | XAI integration (SHAP, LIME) |
| Privacy Preservation | Centralized IDS risks data exposure | Federated learning; differential privacy |

| | | |
|---|---|---|
| Zero-Day Detection | Unknown attacks absent from training data | Unsupervised anomaly detection; novelty detection |
| Benchmark Standardization | Incomparable results across datasets | Community-standard, reproducible benchmarks |

**TABLE 4. Open challenges and prospective research directions.**

Adversarial robustness: ML and DL-based IDS models can be vulnerable to adversarial evasion and poisoning inputs, which motivates adversarial training and the design of certified defenses. Cost-sensitive real-time detection under latency constraints relies on choosing lightweight architectures and model pruning or quantization to efficiently carry out inference on edge devices. Federated IDS robustness and convergence, zero-day attack detection based on unsupervised and novelty-detection approaches and a standardized evaluation framework among heterogeneous benchmark datasets are the most important research agenda.

The heterogeneity of IoT devices from the perception to the application layer complicates the development of a unified detection architecture. Models trained for gateway-class devices can be over-parameterized at the perception layer on resource-constrained MCUs. Conversely, less resource-intensive models at the perception layer may not perform well at the fog and cloud tier. This motivates hierarchical detection architectures where lightweight, heuristic-based or shallow machine learning-based detectors at the edge tolerate benign traffic, while suspicious traffic can be escalated to deep learning or federated models at the fog and cloud layers. Achieving this will require tighter collaboration between the system design and machine learning communities on energy-aware model selection, communication-efficient federated aggregation algorithms, and standardized interfaces to support cross-layer detection escalation.

## 9. CONCLUSION

We envision that the hierarchical architecture we describe can include rule-based and shallow ML-based solutions at the edge (which are likely to have small resource footprints and high interpretability) and deep learning and federated learning at the fog and cloud layer (which are likely to be more expressive and more effective at preserving privacy). We hope this threat-to-countermeasure mapping and comparison will influence the development of more efficient and effective approaches to AI-based intrusion detection in this fast-evolving domain.

This work surveys the landscape of AI-based Intrusion Detection Systems regarding the integrated IoT-cloud stack, i.e., we discuss the architectural stack and its threat landscape. Then we analyse representative attacks in each layer of the perception, network, transport, processing, and application layers and their corresponding AI-based detection solutions, including rule-based, shallow ML-based, or deep learning-based solutions. It also describes the recent literature on federated learning, graph neural networks, transformers, and explainable AI. The analysis suggests that no approach consistently outperforms others across layers and threats. Shallow ML is competitive where data traffic is well classified and when there is limited processing power. Conversely, deep learning (DL) and federated learning generalize better and preserve the privacy of IoT nodes but incur overhead. Data scarcity, adversarial robustness, latency, model transferability, interpretability and benchmark definitions remain open challenges for building resilient, scalable and trustworthy AI-IDS for securing next-generation IoT-cloud systems.

### References


1. H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," J. Netw. Comput. Appl., vol. 36, no. 1, pp. 16–24, Jan. 2013.
2. P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, "A detailed investigation and analysis of using machine learning techniques for intrusion detection in cloud environment," IEEE Commun. Surveys Tuts., vol. 21, no. 2, pp. 1934–1971, 2nd Quart. 2019.
3. F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges," IEEE Commun. Surveys Tuts., vol. 22, no. 3, pp. 1686–1721, 3rd Quart. 2020.
4. S. Zaman, K. Alhazmi, M. A. Aseeri, M. R. Ahmed, R. T. Khan, M. S. Kaiser, and M. Mahmud, "Security threats and artificial intelligence based countermeasures for Internet of Things networks: A comprehensive survey," IEEE Access, vol. 9, pp. 94668–94690, 2021.
5. M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (IoT) security," IEEE Commun. Surveys Tuts., vol. 22, no. 3, pp. 1646–1685, 3rd Quart. 2020.
6. A. Aldweesh, A. Derhab, and A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," Knowl.-Based Syst., vol. 189, Feb. 2020, Art. no. 105124.

7. S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of internet of things (IoT): A survey," J. Netw. Comput. Appl., vol. 161, Jul. 2020, Art. no. 102630.
8. N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2671–2701, 3rd Quart. 2019.
9. T. D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, and A.-R. Sadeghi, "DïoT: A federated self-learning anomaly detection system for IoT," in Proc. IEEE 39th ICDCS, Jul. 2019, pp. 756–767.
10. R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer Internet of Things devices," in Proc. IEEE Secur. Privacy Workshops (SPW), May 2018, pp. 29–35.
11. Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, D. Breitenbacher, A. Shabtai, and Y. Elovici, "N-BaIoT: Network-based detection of IoT BotNet attacks using deep autoencoders," IEEE Pervasive Comput., vol. 17, no. 3, pp. 12–22, Jul. 2018.
12. H. Alaiz-Moreton, J. Aveleira-Mata, J. Ondicol-Garcia, A. L. Muñoz-Castañeda, I. García, and C. Benavides, "Multiclass classification procedure for detecting attacks on MQTT-IoT protocol," Complexity, vol. 2019, Apr. 2019, Art. no. e6516253.
13. N. Moustafa, B. Turnbull, and K.-K. R. Choo, "An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of Internet of Things," IEEE Internet Things J., vol. 6, no. 3, pp. 4815–4830, Jun. 2019.
14. R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," IEEE Access, vol. 7, pp. 41525–41550, 2019.
15. M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," J. Inf. Secur. Appl., vol. 50, Feb. 2020, Art. no. 102419.