SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V13I6P111

Volume 13 Issue 6, 134-144, June 2026

Original Article

A Lightweight Security Decision Framework for IoT Intrusion Detection Using Entropy-Guided Feature Integrity and Adaptive Ensemble Learning

Saif Wali Ali Alsudani, Mohammad-Reza Feizi-Derakhshi*

Computerized Intelligence Systems Laboratory, Department of Computer Engineering, University of Tabriz, Tabriz, Iran.

**Corresponding Author : mfeizi@tabrizu.ac.ir*

Received: 12 March 2026 Revised: 11 April 2026 Accepted: 10 May 2026 Published: 27 June 2026

Abstract *- The rapid growth of the Internet of Things (IoT) has intensified cybersecurity risks while exposing the limitations of traditional security solutions in resource-constrained environments. Intrusion detection in IoT systems, therefore, requires reliable, real-time decision-making with minimal computational overhead. This paper presents a lightweight IoT security decision framework that combines entropy-guided feature selection with an adaptive ensemble-based intrusion detection strategy. The proposed approach employs an entropy–correlation (EnCor) feature selection pipeline to construct a compact and informative feature subset, reducing complexity while preserving discriminative security characteristics. Detection decisions are generated using a soft voting ensemble of complementary machine learning classifiers, supported by an adaptive fallback mechanism to improve reliability under diverse attack scenarios. The framework is specifically designed for edge- and gateway-level IoT deployment, avoiding the high latency and computational demands associated with deep learning and blockchain-based solutions. Experimental evaluation on the TON_IoT and CICIoT2023 datasets demonstrates high detection accuracy with low inference latency and reduced memory consumption. The results confirm that effective intrusion detection can be achieved without compromising practical deployment feasibility. Overall, the proposed framework establishes intrusion detection as an efficient and deployable security decision layer for real-world IoT environments.*

Keywords *- Internet of Things (IoT) Security, Intrusion Detection System (IDS), Entropy-Based Feature Selection, Ensemble Learning, Edge Computing Security.*

1. Introduction

The explosive proliferation of the Internet of Things (IoT) has radically transformed modern computing by overwhelming interconnectedness between physical objects, digital services, and smart applications in the forms of smart home solutions, healthcare systems, industrial automation ecosystems, and smart cities. On the other side of this fast-speed technological development, among cyber security challenges raised by IoT environments, we could also include the interoperability and resource-constrained IoT devices interconnections nearby to a large amount of heterogeneous devices [1]. As these IoT devices are generally low-power and have limited computation ability, memory resources, and energy availability, they become an attractive target for cyberattacks and cannot be protected using traditional security mechanisms [2]. For security, some basic requirements of IoT systems, such as integrity of data, availability of services, confidentiality, and reliability in operation, should be assured. Several types of attacks can cause service unavailability and expose private information, making IoT infrastructures less reliable, including DDoS (Distributed Denial of Service) attacks and other protocol-level intrusion techniques like botnet attacks or spoofing attacks [3]. Traditional security mechanisms are often unsuitable for typical IoT environments because heavyweight cryptographic algorithms impose high computational overhead, centralized architectures increase communication costs, and latency-sensitive IoT applications require lightweight and efficient protection mechanisms [4]. These types of environments require that solutions be both lightweight and effective, running close to the data sources at the edge while keeping detection rates intact [5]. It has been shown that IDS is important for addressing IoT security problems by mon of-the-art Deep Learning (DL)-based IDS methods proposed to date are based on sophisticated DL architectures that incur high memory utilization and computation costs, which restricts their applicability in resource-constrained IoT environments while maximizing detection accuracy. These restrictions on sizes render them unsuitable candidates for real-time, resource-constrained IoT gateways and edge devices. Therefore, rather than focusing just on having a high correctness on detections, on data

collection and computational resources for running the model, we need designs that are decision reliable with real-time precision in an ongoing constrained resource setting [6]. On one hand, other IoT security paradigms have been proposed, such as blockchain-enabled frameworks for achieving data integrity, traceability, and trust management. Currently, while blockchain technologies can help with improving security and transparency, they often also add communication overhead, storage demand, and consensus latency that is not ideal for time-critical IoT applications [7]. In this sense, lightweight and interoperable IDS frameworks allow to build an efficient proactive security layer able to detect at an early stage suspicious activities before they lead to service disruption, infrastructure instability, or data breach [8]. One of the major research challenges is how to design intrusion detection systems capable of providing effective infrastructure protection while satisfying the lightweight operational requirements of IoT environments which can achieve effective infrastructure protection based on light weight operational requirements in IoT based environments.

In order to tackle these challenges, this paper proposes a lightweight IDS framework based on entropy-guided feature selection combined with an adaptive ensemble classification strategy [9, 10]. Under such a dimension reduction framework, the aim is to reduce the input data complexity but at the same time retain discriminative security information in order to detect attacks. Specifically, we employ correlation-aware filtering together with entropy-based relevance analysis to construct a compact feature subset that is informative enough for IoT traffic data. The second aspect is the combination of detection decisions, which are performed using a soft voting ensemble of complementary lines of ML classifiers, making more reliable decisions and hence reducing false positives that do not require deep learning, which can be expensive to run. The experiment uses datasets from TON_IoT and CICIoT2023, generated in advance, which emulate diverse attack behaviors at the network layer and application layer to evaluate the performance of the proposed algorithm. The experimental results show that the proposed framework is able to achieve high accuracy, compared with conventional intrusion detection methods, and various IoT-based environments contain low CPU power and limited memory consumption.

1.1. The Main Contributions of this Work can be Summarized as Follows

- A lightweight entropy-guided feature selection mechanism tailored to IoT security requirements through relevance analysis and correlation-aware redundancy reduction.
- A robust ensemble-based security decision engine supported by an adaptive fallback strategy to improve decision reliability under dynamic IoT traffic conditions.
- A comprehensive experimental evaluation demonstrating that effective intrusion detection can be achieved without sacrificing computational efficiency, low-latency operation, or deployment feasibility in resource-constrained IoT environments.

In summary, this work positions intrusion detection as a practical and reliable security decision-making layer rather than merely a conventional classification task, thereby supporting efficient and trustworthy IoT security operations within resource-constrained environments.

2. Related Work

With the increased growth of the Internet of Things (IoT) systems, many researchers have focused on implementing Intrusion Detection Systems (IDSs) suitable for constrained computational and energy resources. The existing literature can then be categorized into (1) machine learning–based IDSs, (2) lightweight feature selection frameworks, (3) ensemble-based detection strategies, and (4) blockchain-based IoT security solutions.

2.1. IoT Intrusion Detection Using Machine Learning

Several works implemented traditional machine learning algorithms, specifically Support Vector Machines, Random Forests, k-Nearest Neighbors, and boosting classifiers to detect attacks in IoT environments [11, 12]. More recently, several deep learning–based IDSs, such as CNN-, RNN-, and LSTM-based architectures, were proposed to capture temporal dependencies in network traffic. Although their detection performances are superior, the dimensionality of the utilized feature sets and the complexity of deep architectures make them less practical for deployment in resource-constrained IoT and edge devices because of increased inference latency and memory utilization [13, 14]. Recently, [15] proposed a privacy-preserving federated learning IDS framework using lightweight neural networks with Differential Privacy and Homomorphic Encryption mechanisms.

2.2. Lightweight and Feature-Selection-Based IDS Frameworks

To alleviate performance degradation, several lightweight IDS architectures have integrated feature selection and dimensionality reduction methods such as Information Gain, ReliefF, Linear Discriminant Analysis (LDA), and Recursive Feature Elimination (RFE) [16, 17]. These techniques are designed to reduce computational cost while maintaining acceptable intrusion detection performance. The majority of the current methods generally consider feature relevance ranking and ignore Redundancy Reduction (RR) and the semantic context information security relevance, which may lead to undesired intrusion detection robustness and interpretability in a decision-making task [18]. Recently, [19] proposed a Firefly Algorithm optimized hybrid deep learning framework for intrusion detection in IoT environments. The study demonstrated high detection accuracy through optimized feature selection and hybrid deep learning; however, the framework still depends on computationally

intensive architectures that may limit lightweight edge deployment feasibility.

2.3. Ensemble-Based and Adaptive IDS Approaches

To improve the robustness and generalization capability of IDS frameworks, several ensemble learning approaches, such as hard voting and soft voting, have been investigated for IoT intrusion detection and edge-based security environments [20, 21]. Ensemble methods integrate multiple classifiers to reduce the limitations of individual learners and improve detection reliability. However, most ensemble-based IDS frameworks remain static and do not contain adaptive fallback mechanisms capable of maintaining stable performance under dynamic IoT traffic conditions [22].

Recently, [23] proposed a lightweight and efficient intrusion detection framework for resource-constrained IIoT environments. The framework demonstrated high detection accuracy while maintaining low computational overhead suitable for edge deployment. Although the framework demonstrated strong detection performance, maintaining lightweight deployment and computational efficiency remains a critical challenge in large-scale IIoT environments.

2.4. Blockchain-Oriented IoT Security Models

Blockchain-oriented IoT security frameworks have been proposed to preserve transparency, data integrity, and decentralized trust management. These mechanisms improve accountability and tamper resistance; however, they may also introduce additional communication, storage, and computational overhead in resource-constrained IoT environments [24, 25]. Such limitations may negatively affect the real-time operation of anomaly-based intrusion detection systems and reduce their deployment feasibility in IoT edge gateways and large-scale distributed environments. Furthermore, integrating blockchain mechanisms with privacy-preserving security frameworks remains challenging due to the trade-off between operational efficiency, scalability, and security robustness in practical IoT deployments.

2.5. Research Gap and Proposed Contribution

Although the literature review above shows that previous IoT IDS solutions primarily aim to attain a sufficiently high accuracy of their approaches in return for overlooking the feasibility of deploying it, or that they opt to make decisions based on low computational cost algorithms which inherently lack robustness and trustworthiness [26]. Many of them have high memory consumption, communication network overhead, and computation complexity, which may limit their infrastructure for practical implementations in IoT edges, either based on deep learning or privacy [27, 28]. Moreover, many ensemble-based IDS frameworks do not include adaptive reliability mechanisms capable of maintaining stable performance under dynamic IoT attack conditions.

This paper addresses these limitations by proposing a lightweight security decision framework that integrates entropy-guided relevance analysis, correlation-aware redundancy filtering, ensemble-based decision trust, and an adaptive fallback strategy for real-time and resource-constrained IoT edge environments.

Recent IoT intrusion detection frameworks using deep learning, federated learning, ensemble learning, and blockchain-oriented security mechanisms have presented promising detection performances as detailed in Table 1. Nonetheless, many of the approaches reported and implemented at this moment come with high computation complexity or operation overhead when applied in a resource-constrained IoT environment. In contrast, with the proposed EnCor + Adaptive SVE framework, high detection accuracy is realized while remaining light-weight operation and extreme feasibility to edge deployment, which may be more applicable for real-world applications such as IoT security.

Table 1. Comparison of recent IoT intrusion detection frameworks

Ref.	Dataset	Core Method	Accuracy (%)	Edge Feasibility
[15]	IoT-ID	FL + DP + HE	93.5	Moderate
[19]	NF-BoT-IoT-v2, IoTID20	FA-CNN-RNN	99.9 / 98.2	Moderate
[20]	Bot-IoT, CICIDS2018, NSL-KDD, IoTID20	Ensemble IoT-Edge IDS	98.8	Good
[23]	CIC-IDS2017, CSE-CIC-IDS2018, CIC-DDoS2019	ROSE-BOX Lightweight IDS	>99.85	High
Proposed	TON_IoT, CICIoT2023	EnCor + Adaptive SVE	99.83	High

3. Methodology

3.1. Overview of the Proposed Lightweight IDS Framework

The proposed approach is organized as a very lightweight security decision model for operation at the IoT gateways and edge nodes, the vicinity of which plays an important role in accurate and timely intrusion detection, as can be seen in Figure 1. The architecture is modular and supports early threat detection and symptom mitigation with low latency and computational overhead. This paper introduces an end-to-end process that includes information security-aware feature selection, ensemble optimization, and decision-making stages, in which each stage is mutually

enforcing not only the protection of security-related info boxes but also the resilience and trustworthiness of intrusion decisions under a varying IoT context. Furthermore, the framework operates as an implementation agnostic plug-and-play template for scalable heterogeneous IoT context environments, which has become a growing challenge since dynamic high-dimensional data needs to be experience-aware but acceptable by all present participants, enabling trustful detection. By combining efficient feature determination and light-weight training rules, we maintain the speed from diagnosis to decision, but with much less computation effort in edge point.

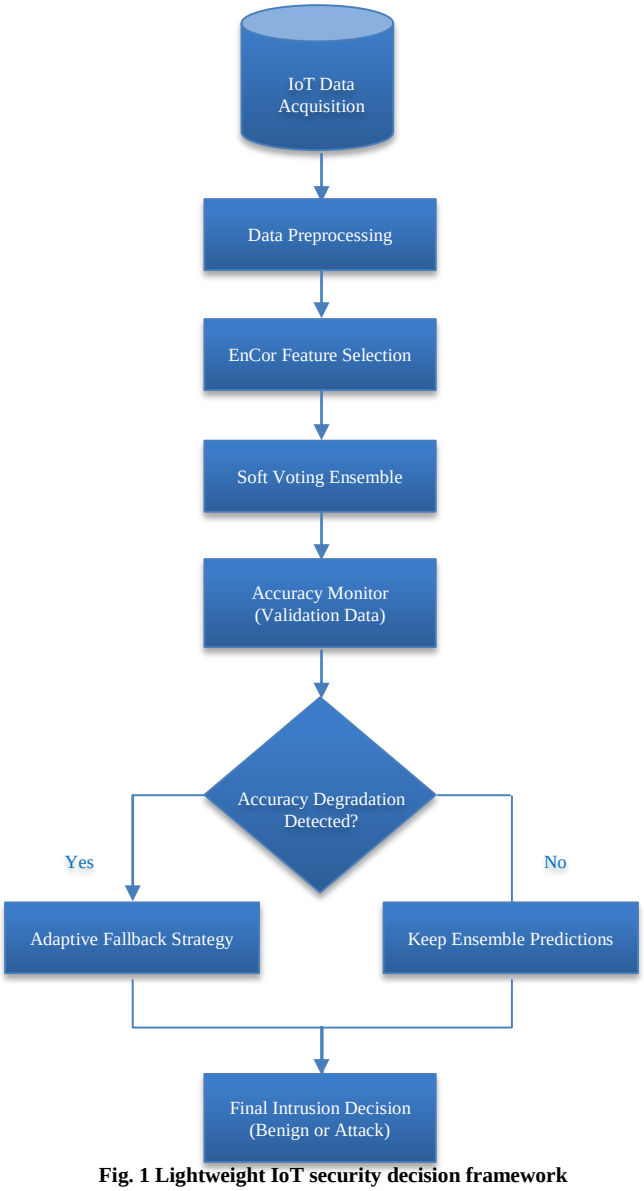

Fig. 1 Lightweight IoT security decision framework

3.2. Dataset Selection and Preprocessing

Important from a security perspective, the dataset used is pivotal, and preprocessing was explained to contribute to presenting accurate decisions and the robustness of the IDS. In this work, experimental results on two very genuine datasets (TON_IoT and CICIoT2023) to verify the proposed approach since they cover many real IoT attacks both in the network and application layer at a large scale. Due to the diversity of threats represented in these two datasets, they are also suitable for measuring the security efficiencies of lightweight IDS methods [29, 30]. In the above context, filtering noise and reducing class imbalance bias is treated as a preventive operation known as "pre-processing," which also coarsens ID decisions with respect to robustness. The smart IoT traffic logs are pre-processed into clean, normalized, and encoded features with a balance check to prevent over-distorting of the security meaning pattern. By preprocessing the input data before analysis, such pre-processing brings into play operator decisions based on true suspiciousness in place of artifacts or incompleteness pertaining to, but not limited to, the same dataset.

3.3. Threat Model and System Design Assumptions

This subsection formalizes an outline of the relevant security boundaries, adversarial capabilities, and deployment assumptions considered in this work. The proposed IDS targets over heterogeneous and resource-constrained IoT environments facing several internal and external threats, such as passive activities like traffic monitoring, and active actions like injection, flooding, spoofing, and scanning. To provide a uniform assessment of the security, the categories of threats they are exposed to, surfaces that can be attacked, and assumptions made regarding system monitoring are listed concisely in Table 2, Tim Real-Time Multi-Sensor Fusion Process for Edge Gateway Security Evaluation Figure 2. These features, read together, define the working model of the intrusion detection system and determine how to mimic decisions taken in real-life IoT deployments [31].

Table 2. Threat model and system assumptions

Aspect	Description
Environment	Resource-constrained IoT networks operating through edge gateways.
Adversary	Internal and external attackers are launching passive and active attacks.
Attack Surface	Network flows and protocol-level traffic behavior.
Attack Types	Scanning, spoofing, flooding, botnet, and DoS activities.
Monitored Data	Flow-based IoT traffic from TON_IoT and CICIoT2023 datasets.
Trust Assumption	Edge gateway is trusted; IoT devices may be compromised.
Objective	Early detection of malicious behavior with low latency.
Constraints	Limited memory, computation, and real-time response needs.

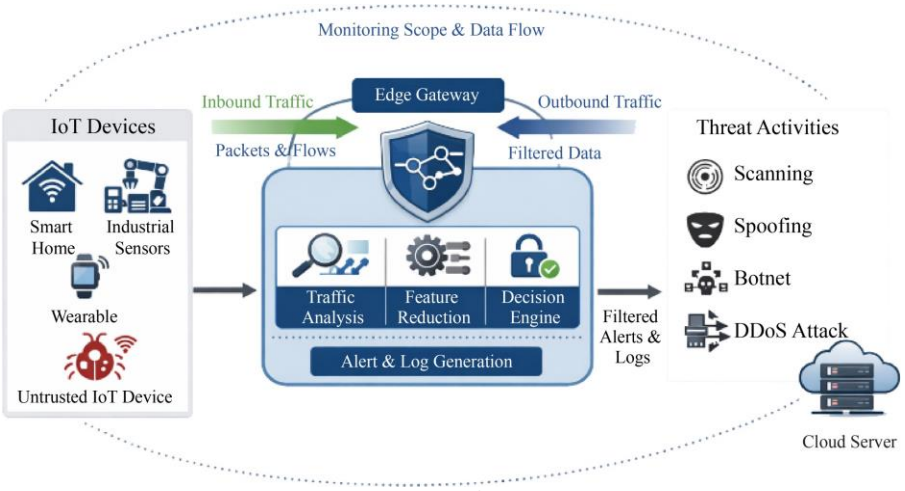

Fig. 2 Monitoring scope and data flow at the IoT edge gateway

3.4. Entropy–Correlation-Based Feature Selection (EnCor)

To our knowledge, the pipeline proposed herein leverages on an Entropy–Correlation (EnCor) feature selection framework to obtain a computationally efficient and robust detection process. Therefore, this amalgamation of these security features will dichotomize the relevant traits through information gain and then eliminate redundancy, maintaining only the sorting feature set, which provides a space as far as compactness is concerned [32].

Figure 3 Inter-feature dependencies, which motivate correlation-aware pruning. In Table 3, the last eGEM subset (EnCor) is reported, while in Table 4, its semantic interpretations.

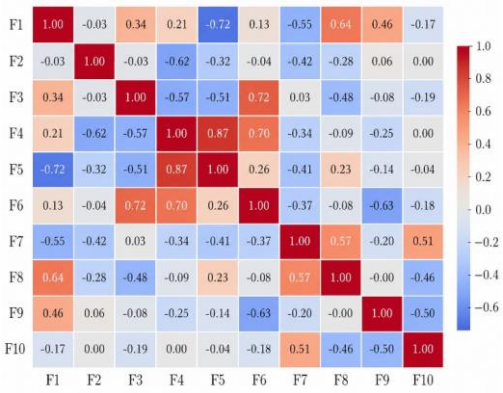

Fig. 3 Correlation heatmap of IG-ranked features before redundancy filtering

Table 3. Final ENCOR feature subset after correlation filtering

Feature Name	IG Rank	Correlation Status	Included in EnCor
src_ip_packets_rate	1	Low redundancy	Yes
dst_port	2	Low redundancy	Yes
flow_duration	3	Low redundancy	Yes
total_forward_packets	4	High correlation	No
packet_length_stddev	5	Low redundancy	Yes
avg_packet_size	6	High correlation	No
tcp_flag_count	7	Low redundancy	Yes
protocol_type	8	Low redundancy	Yes
init_win_bytes_forward	9	Low redundancy	Yes
flow_bytes_per_sec	10	Low redundancy	Yes

Table 4. Semantic interpretation of retained ENCOR features

Feature Name	Interpretation
src_ip_packets_rate	High values indicate flooding or scanning activity.
dst_port	Repeated access may reflect service exploitation.
flow_duration	Abnormal lengths suggest attack behavior.
packet_length_stddev	High variance may indicate evasion or manipulation.
tcp_flag_count	Irregular flags relate to spoofing or SYN attacks.
protocol_type	Certain protocols are more prone to IoT attacks.
init_win_bytes_forward	Irregular window sizes suggest anomalous sessions.
flow_bytes_per_sec	Extreme rates indicate volumetric or stealth attacks.

3.5. Classification Models and Ensemble Strategy

To sum it up, the classification stage serves as a security decision engine that converts the observed IoT traffic patterns into benign or intrusion decisions. The architecture relies on multiple complementary models instead of a single decision maker and gives probabilistic outputs, which can be aggregated to enhance the trustworthiness of a decision. We conjecture that on the one hand, an ensemble-based approach can supply better immunity from common individual learning bias whilst retaining their robustness and simultaneously could be able to act as a more potent resilient mechanism towards numerous attack patterns, to the benefit of improving the system robustness [33].

3.6. Security Decision Engine with Adaptive Fallback

At the same time, the security decision engine must also integrate an Adaptive Fallback pyramid in the framework to maintain higher operational reliability. As illustrated in Figure 4, the validity accuracy is tracked continuously, and if the ensemble performance monitored by this criterion drops beyond specific limits, it falls back to its most trusted base classifier.

This design makes the proposed IDS self-healing by recovering from transient drops in ensemble reliability without human intervention or retraining. This strategy not only prevents decision failure on time-varying traffic problems but also guarantees stable detection performance in dynamic IoT environments.

By prioritizing positive selection security metrics in accordance with traffic shapes offered at the time, our proposed IDS framework achieves a trade-off to be generic and directive across multiple dimensions that is also practical for real-world implementation in resource-constrained IoT systems.

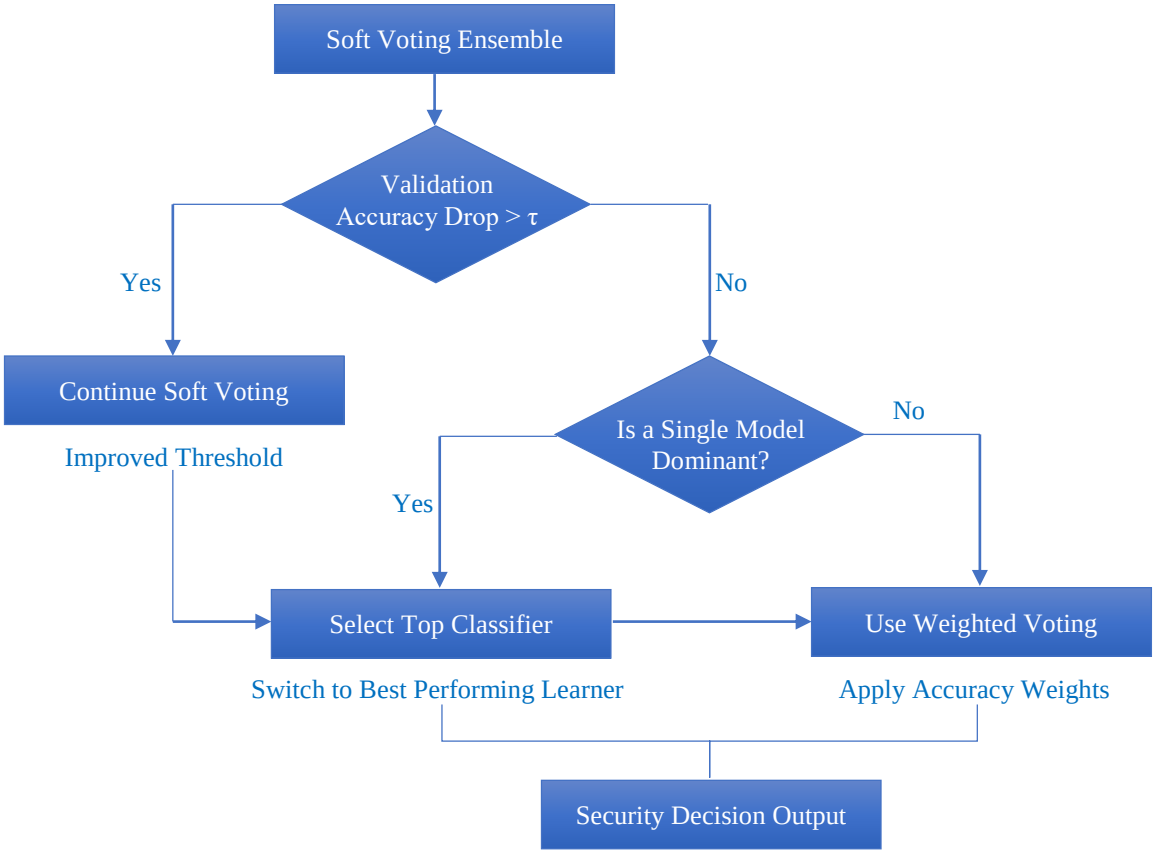

Fig. 4 Adaptive fallback strategy for reliable ensemble-based intrusion detection

3.7. Evaluation Metrics and Validation Strategy

In order to find the feasibility of using it on time on IoT edge-based systems, we have evaluated the detection accuracy and computational efficiency of our proposed IDS framework. The performance is evaluated against apps using the generic classification metrics Accuracy, Precision, Recall, F1-score, and AUC-ROC, taken along with profiling memory nature in the experimental results based on speed of detection, training time, and inference latency for deployability check. You could use the p -value from the paired t -test between competing models to measure statistical significance, so you can confirm any performance improvement is attributable solely to chance.

Evaluation metrics are defined as follows:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

$$\text{Precision} = \frac{TP}{TP+FP}, \text{Recall} = \frac{TP}{TP+FN} \quad (2)$$

$$F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (3)$$

$$t = \frac{\bar{d}}{s_d/\sqrt{n}} \quad (4)$$

where TP, TN, FP, and FNrepresent true positives, true negatives, false positives, and false negatives, respectively, and $\bar{d}$and $s_d$denote the mean and standard deviation of paired performance differences across folds.

4. Results and Discussion

This section evaluates the effectiveness and practicality of the proposed entropy-guided lightweight intrusion detection framework and discusses its implications for real-world IoT security deployment.

4.1. Detection Performance

The proposed IDS was also evaluated according to accuracy, precision, recall, F1-score, and AUC-ROC metrics over the TON_IoT and CICIoT2023 datasets as presented in Table 5.

The particular confusion matrix of Figures 5 and 6 presents the classification results for TON IoT and CICIoT2023, respectively, giving a detailed view of class-wise prediction performance.

Table 5. Detection performance on TON_IoT and CICIoT2023 datasets

Dataset	Model	Accuracy (%)	AUC	Recall (%)	F1-score (%)
TON_IoT	Logistic Regression (LR)	98.74	0.987	98.55	98.58
	Random Forest (RF)	99.12	0.991	99.08	99.05
	Gradient Boosting (GB)	99.36	0.993	99.31	99.29
	Soft Voting Ensemble (SVE)	99.71	0.997	99.69	99.67
	SVE + Adaptive Fallback	99.83	0.998	99.81	99.79
CICIoT2023	Logistic Regression (LR)	97.62	0.972	97.31	97.39
	Random Forest (RF)	98.11	0.981	98.02	97.99
	Gradient Boosting (GB)	98.47	0.985	98.29	98.31
	Soft Voting Ensemble (SVE)	98.89	0.989	98.81	98.78
	SVE + Adaptive Fallback	99.12	0.991	99.08	99.05

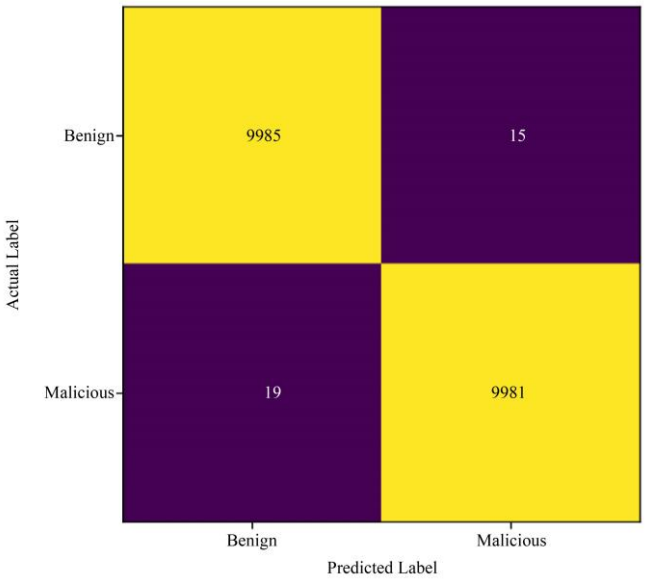

Fig. 5 Confusion matrix for TON_IoT dataset

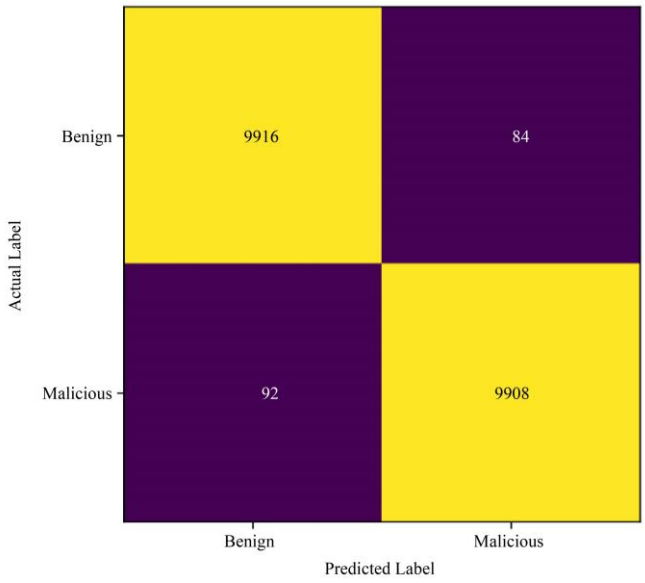

Fig. 6 Confusion matrix for CICIoT2023 dataset

The SVE + Adaptive Fallback model demonstrates very stable performance while only a few others misclassified on both datasets, indicating good separation of normal and attack traffic. Our non-hybrid voting-based ensemble scheme outperforms any of the classifiers individually and achieves detection rates higher than 99%.

Besides, the stability of confusion patterns shows that the model is robust to class imbalance and varying attacker distributions. The small gap between precision and recall confirms the balanced learning property, which does not favor dominant classes. The high AUC-ROC values indicate that attack traffic can be well separated from normal traffic under diverse network conditions. All these results in combination, exhibit the strength and applicability of the proposed IDS in diverse IoT systems. In addition, the universal enhancements achieved in both datasets further demonstrate the portability of our framework to other IoT platforms. The small variances of performance measures for folds also indicate that the model is dependable in repeated experiments.

4.2. Computational Efficiency

All methods were assessed with respect to the possibility of deployment on IoT edge, by analysing their training time required, the inference latency, and memory overhead. The data is presented in Table 6.

Despite that the proposed framework comprises multiple base learners, the inference latency is less than 1 ms on both datasets , suggesting that it can still be deployed in real-time over IoT gateways without GPU acceleration. The modest memory utilization also suggests that the demonstrated IDS achieves a practical trade-off of detection reliability and operational efficiency.

Table 6. Computational efficiency on TON_IoT and CICIoT2023 datasets

Dataset	Model	Training Time (s)	Inference Latency (ms)	Memory Usage (MB)
TON_IoT	Logistic Regression	2.84	0.41	46
	Random Forest	4.12	0.63	71
	Gradient Boosting	4.87	0.78	78
	Soft Voting Ensemble	6.35	0.92	91
	SVE + Adaptive Fallback	6.82	0.95	94
CICIoT2023	Logistic Regression	3.1	0.47	49
	Random Forest	4.48	0.69	75
	Gradient Boosting	5.23	0.83	82
	Soft Voting Ensemble	6.88	0.96	96
	SVE + Adaptive Fallback	7.15	0.98	99

4.3. Statistical Validation

Using stratified 10-fold cross-validation, the statistical significance of the performance improvements is assessed using paired t-tests. The results in Table 7 show that the ensemble with adaptive Fallback clearly outperforms even the best of the individual classifiers, so one can be sure this is not just random variation. Additionally, the consistently low p-values (statistically significant) that are obtained from both datasets denote reliability and repeatability of the proposed IDS framework.

Table 7. Paired T-Test results for performance comparison (10-fold cross-validation)

Dataset	Comparison	Mean Difference (Accuracy)	Std. Dev.	t-Statistic	p-Value
TON_IoT	SVE + Fallback vs LR	1.09	0.18	19.21	0.0001
	SVE + Fallback vs RF	0.71	0.15	15.01	0.0001
	SVE + Fallback vs GB	0.47	0.12	12.39	0.0002
CICIoT2023	SVE + Fallback vs LR	1.5	0.22	21.5	0.0001
	SVE + Fallback vs RF	1.01	0.19	16.82	0.0001
	SVE + Fallback vs GB	0.65	0.17	12.15	0.0003

4.4. Comparative Analysis with Recent IDS Frameworks

Table 8 compares the proposed framework with other recent IoT and IIoT intrusion detection methods [34-38]. With new research works around feature selection, ensemble learning, and deep learning techniques, the intrusion detection performance in IoT environments is significantly improved. In [34], CNN–LSTM–based feature reduction was used with SVM and Random Forest classifiers on the TON_IoT dataset, and [35] proposed QRIME-based feature minimization alongside a stacked deep polynomial network on

CICIoT2023. In the same spirit, lightweight behavior–driven feature selection methods are proposed with a light complexity to enhance generalization as [36]. Even the IDS frameworks based on Deep Learning has shown high detection. The study [37] proposed an improved LSTM framework that achieved high-level intrusion detection accuracy on multiple benchmark datasets, including CICIoT2023. Additionally, [38] implemented a multi-layered AI architecture that combines the technologies of Graph Neural Networks, Transformer encoders, reinforcement learning, and federated learning to enhance scalability and attack mitigation performance under software-defined IoT environments. The proposed framework achieves comparable results on intrusion detection while alleviating computational load and deployment limitations with respect to these approaches for a lightweight IoT edge environment. Combining the analysis of integrity w.r.t soft feature importance guided by entropy with adaptive learning through an ensemble classifier based on soft voting allows for reliable intrusion detection performance while achieving low computational overhead and operation below latency threshold – suitable to fit within resource-constrained IoT deployments.

Table 8. Comparison of the proposed framework with recent IoT intrusion detection studies

Ref.	Dataset	Core Method	Accuracy (%)	Edge Feasibility
[34]	TON_IoT	CNN-LSTM + SVM/RF	98.00	Moderate
[35]	CICIoT2023	QRIME-SDPN	99.20	Moderate
[36]	TON_IoT	Hybrid Feature Selection + Ensemble Learning	98.60	High
[37]	CICIoT2023, NSL-KDD, UNSW-NB15	Enhanced LSTM (E-LSTM)	>95.00	Moderate
[38]	CICIoT2023, TON_IoT, Edge-IIoTset	GNN + Transformer + PPO	98.70	Limited
Proposed	TON_IoT, CICIoT2023	EnCor + Adaptive SVE	99.83	High

4.5. Discussion

The experimental results indicate that the proposed lightweight IDS effectively detects intrusions in IoT environments while preserving a suitable trade-off between detection performance and computational efficiency. Our high F1-scores on the TON_IoT dataset and competitive performance on CICIoT2023 also show that threat detection can be made through lightweight approaches, without relying on computational intensive deep learning architectures. Compared with many CNN-, LSTM-, and Transformer-based IDS frameworks, the proposed model achieves superior test accuracy (very strong detection capability) within a reduced inference latency and modest memory utilization under the constraints of lightweight IoT edge deployment capability.

Our entropy-guided feature selection mechanism refines the information by retaining the most relevant and clean security-related information among different network traffic conditions, thus improving robustness be removing irrelevant/noisy features. At the same time, this reduced feature set ensures more compact global representations and, therefore, a simpler model capable of retaining most relevant evidence needed to detect intrusions in resource-constrained IoT environments.

In addition, the soft voting ensemble approach strengthens decision confidence through pooling heterogeneous classifiers with complementary roles, thus minimizing the limitation of a single learning model. Consequently, the proposed framework successfully obtains stable and balanced detection performance in the face of heterogeneous IoT traffic patterns.

In addition, the adaptive fallback mechanism mitigates performance degradations and preserves detection reliability against a wide variety of network traffic patterns and evolving techniques of attack. The model can maintain operational stability by adopting the classifier with the best performance (i.e., highest confidence output) rather than a static ensemble solution used in traditional ensemble IDS frameworks when overall confidence drops. In terms of a system perspective, the proposed solution can be taken as an active-light intrusion detection layer vis-a-vis traditional IoT security solutions such as crypto-based protection and blockchain-related integrity preservation mechanisms. The framework is also a practical candidate for real-world deployment to IoT settings such as smart homes, industrial IoT systems, healthcare infrastructures, and mission-critical edge applications because of its lightweight structure, low-latency execution, and modest resource usage.

5. Conclusion

This paper outlined an entropy-guided, efficient intrusion detection framework to deliver accurate and real-time security across IoT environments. The proposed framework augments information entropy with correlation-aware feature reduction to retain security-relevant data at minimum computational cost. The soft voting ensemble significantly enhances the

dependability of decision-making, while an adaptive fallback mechanism provides resilient detection performance in dynamically changing network traffic scenarios. Experimental evaluation on the two used datasets, TON_IoT and CICIoT2023, demonstrated that the proposed framework reaches high detection accuracy & F1− scores with low inference latency while consuming moderate memory space. Such properties make the framework ready to migrate and deploy on IoT gateways and edge-based environments without requiring GPU-supported infrastructure. The proposed IDS, moreover, is different from computation-heavy deep learning frameworks and communication-intensive blockchain-based security-aggregation models as it aims to balance detection reliability, operational efficiency, and deployment feasibility of Resource-Constrained IoT systems.

Future work will focus on extending the framework to multi-class attacks categorization, increasing robustness to adversary traffic patterns, and deploying the model in real-world IoT testbeds for performance evaluation in operational conditions close enough to practical deployment. Also, future works could consider and reach a federated and explainable intrusion detection in order to enhance privacy preservation, transparency, and trustworthiness among distributed IoT ecosystems. In addition, lightweight optimisation algorithms and adaptive edge intelligence mechanisms will also be examined to develop the scalability, energy efficiency, and real-time detection capability in resource-constrained environments.

References

[1] Menachem Domb, and Yehuda Shnaps, *Cybersecurity Threats and Mitigations Related to Smart Cities Operation*, Smart Cities – Foundations and Perspectives, IntechOpen, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[2] Oyeniyi Akeem Alimi, "Data-Driven Learning Models for Internet of Things Security: Emerging Trends, Applications, Challenges and Future Directions," *Technologies*, vol. 13, no. 5, pp. 1-29, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[3] Amir Pakmehr et al., "DDoS Attack Detection Techniques in IoT Networks: A Survey," *Cluster Computing*, vol. 27, pp. 14637-14668, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[4] Indu Radhakrishnan, Shruti Jadon, and Prasad Honnavalli, "Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices," *Sensors*, vol. 24, no. 12, pp. 1-19, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] Faeiz Alserhani, "Intrusion Detection and Real-Time Adaptive Security in Medical IoT Using a Cyber-Physical System Design," *Sensors*, vol. 25, no. 15, pp. 1-26, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[6] Huma Gupta, Akshay Jadhav, and Abhay Singh Bisht, "Comparative Analysis of Machine and Deep Learning Models for Intrusion Detection in Fog-Enabled IoT Networks," *International Journal of Networked and Distributed Computing*, vol. 14, pp. 1-18, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[7] Cagatay Korkuc et al., "BBNAC: Blockchain Based Network Access Control for IT/OT Infrastructures," *Journal of Network and Systems Management*, vol. 34, pp. 1-34, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[8] Zainab Alwaisi et al., "Securing Constrained IoT Systems: A Lightweight Machine Learning Approach for Anomaly Detection and Prevention," *Internet of Things*, vol. 28, pp. 1-20, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[9] Huiyao Dong, and Igor Kotenko, "A Lightweight and Robust Approach to IoT Intrusion Detection based on Ensemble Deep Learning," *International Journal of Parallel, Emergent and Distributed Systems*, pp. 1-21, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[10] Aya G. Ayad, Nehal A. Sakr, and Noha A. Hikal, "A Hybrid Approach for Efficient Feature Selection in Anomaly Intrusion Detection for IoT Networks," *Journal of Supercomputing*, vol. 80, pp. 26942-26984, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Salam Fraihat et al., "Intrusion Detection in Industrial Internet of Things Network using Feature Optimization and Hybrid Deep Learning," *Discover Internet of Things*, vol. 6, pp. 1-48, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[12] A. Termanini et al., "Using Machine Learning to Detect Network Intrusions in Industrial Control Systems: A Survey," *International Journal of Information Security*, vol. 24, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[13] P. L. S. Jayalaxmi et al., "Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A Survey," *IEEE Access*, vol. 10, pp. 121173-121192, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] C. Rajathi, and P. Rukmani, "Hybrid Learning Model for Intrusion Detection System: A Combination of Parametric and Non-Parametric Classifiers," *Alexandria Engineering Journal*, vol. 112, pp. 384-396, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[15] A. Puviarasu, and V.K. Sudha, "Enhanced IoT Security: Privacy-Preserving Federated Learning Model for Accurate, Real-time Intrusion Detection across Devices," *Ain Shams Engineering Journal*, vol. 17, no. 1, pp. 1-18, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[16] Dainan Zhang et al., "A Lightweight IoT Intrusion Detection Method based on Two-Stage Feature Selection and Bayesian Optimization," *AIMS Electronics and Electrical Engineering*, vol. 9, no. 3, pp. 359-389, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[17] Naveen Saran, and Nishtha Kesswani, "An Analytics-driven Framework for Securing Industrial IoT-Enabled Supply Chain Management Systems," *Supply Chain Analytics*, vol. 11, pp. 1-11, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[18] Abdulla Amin Aburomman, Marwan Alakhras, and Mamun Bin Ibne Reaz, "Leakage-Safe IoT Intrusion Detection with White Shark Optimizer-based Feature Selection," *Array*, vol. 30, pp. 1-10, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[19] Samar M. Zayed, Samah Alshathri, and Walid El-Shafai, "Firefly Algorithm Optimized Hybrid Deep Learning Framework for Intrusion Detection in IoT Environments," *International Journal of Computational Intelligence Systems*, vol. 19, pp. 1-33, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[20] Abdulaziz Aldaej et al., "Ensemble Technique of Intrusion Detection for IoT-Edge Platform," *Scientific Reports*, vol. 14, pp. 1-16, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[21] G. Logeswari et al., "An Improved Synergistic Dual-Layer Feature Selection Algorithm with Two Type Classifier for Efficient Intrusion Detection in IoT Environment," *Scientific Reports*, vol. 15, pp. 1-21, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[22] N. Satheesh Kumar et al., "Swarm-based Intelligent Models for Developing Cybersecurity Frameworks with IDS," *Scientific Reports*, vol. 16, pp. 1-32, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[23] Silin Peng et al., "ROSE-BOX: A Lightweight and Efficient Intrusion Detection Framework for Resource-Constrained IIoT Environments," *Applied Sciences*, vol. 15, no. 12, pp. 1-23, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[24] Khawla Shalabi, Qasem Abu Al-Haija, and Mustafa Al-Fayoumi, "A Blockchain-based Intrusion Detection/Prevention Systems in IoT Network: A Systematic Review," *Procedia Computer Science*, vol. 236, pp. 410-419, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[25] Arbia Riahi Sfar et al., "A Roadmap for Security Challenges in the Internet of Things," *Digital Communications and Networks*, vol. 4, no. 2, pp. 118-137, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[26] Yuqiang Wu, Bailin Zou, and Yifei Cao, "Current Status and Challenges and Future Trends of Deep Learning-Based Intrusion Detection Models," *Journal of Imaging*, vol. 10, no. 10, pp. 1-25, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[27] Hessah A. Alsalamah, and Walaa N. Ismail, "A Swarm-Based Multi-Objective Framework for Lightweight and Real-Time IoT Intrusion Detections," *Mathematics*, vol. 13, no. 15, pp. 1-32, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[28] Alyazia Aldhaheri et al., "Deep Learning for Cyber Threat Detection in IoT Networks: A Review," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 110-128, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[29] Shereen Ismail, Salah Dandan, and Ala'a Qushou, "Intrusion Detection in IoT and IIoT: Comparing Lightweight Machine Learning Techniques Using TON_IoT, WUSTL-IIOT-2021, and EdgeIIoTset Datasets," *IEEE Access*, vol. 13, pp. 73468-73485, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[30] M. Arivukarasi et al., "Federated Autoencoder IDS for IoT: A Fed-ANIDS Approach using CICIoT2023," *Systems and Soft Computing*, vol. 8, pp. 1-14, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[31] Ashish K. Sharma et al., *Securing IoT Environments: Deep Learning-Based Intrusion Detection*, Deep Learning for Intrusion Detection: Techniques and Applications, Wiley, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[32] Gede Teguh Satya Dharma et al., "Weighted ANOVA and Mutual Information for Enhanced Intrusion Detection System," *KINETIK: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, vol. 11, no. 1, pp. 113-122, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[33] Babatunde Olanrewaju-George, and Bernardi 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, pp. 1-10, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[34] Elijah Mwandata Maseno, Zenghui Wang, and Yanxia Sun, "Performance Evaluation of Intrusion Detection Systems on the TON_IoT Datasets Using a Feature Selection Method," *Proceedings of the 2024 8th International Conference on Computer Science and Artificial Intelligence*, Beijing China, pp. 607-613, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[35] Srinivas Cheekati et al., "Intelligent Cybersecurity for IoT: A Hybrid QRIME-SDPN Approach for Network Attack Detection on CIC-IoT-2023," *2025 13th International Conference on Smart Grid (icSmartGrid)*, Glasgow, United Kingdom, pp. 774-781, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[36] N. Dharini, V. S. Janani, and Jeevaa Katiravan, "Efficient Detection of Intrusions in TON-IoT Dataset using Hybrid Feature Selection Approach," *Scientific Reports*, vol. 16, pp. 1-29, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[37] Gaurav Meena, and Ajay Indian, "IDS-IoT: Intrusion Detection System for the Internet of Things Using Enhanced Long-Short Term Memory," *Artificial Intelligence and Applications*, Online First, pp. 1-18, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[38] Jamal Alotaibi, "AI-driven Intrusion Detection and Mitigation Framework for Software-defined IoT Networks," *Peer-to-Peer Networking and Applications*, vol. 18, 2025. [CrossRef] [Google Scholar] [Publisher Link]