KAPS INITIATIVE

Savannah Journal of Science and Engineering Technology
Volume: 04; Issue: 01; Pages: 023-033; 2026.
http://kaacpub.com/index.php/SAJSET/index

DOI: xx.xxxx.x/sajset-04-2026-0090

SAJSET
ISSN:
2992-3581

AI enhanced intrusion detection system for IoT networks using lightweight machine learning model

[1]Disina, A. H., [2]Yunusa A. A., [1]Mohammad N., [3]Abubakar H. and [4]Adamu, A.
[1]*Cyber Security Department, Nigerian Army University Biu, Borno State, Nigeria*
[2]*Computer Science Department, Nigerian Army University Biu, Borno State, Nigeria*
[3]*Department of Electronics and Telecommunication Engineering, Air Force Institute of Technology, Kaduna State, Nigeria*
[4]*Department of Information System, Nigerian Army University Biu, Borno State, Nigeria*
amirahmad22@naub.edu.ng, muhdbaba@gmail.com, hashimubukar@gmail.com, ningi2200@naub.edu.ng

Paper History
Received: 1st October, 2025
Accepted: 20th Nov., 2025
Published: December, 2025

Corresponding author
Disina, A. H.
disina.hassan@naub.edu.ng

Abstract:
The rapid growth of the Internet of Things (IoT) has created significant security challenges because most IoT devices have limited processing power, memory, and energy. This study addresses these issues by developing a lightweight, AI-enhanced intrusion detection system (IDS) tailored for resource-constrained IoT environments. The system emphasizes efficiency, scalability, and real-time detection using lightweight machine learning methods. Using the CIC-IoT 2023 dataset, the researchers built and evaluated models based on Decision Tree and Random Forest algorithms. Data preprocessing, training, and evaluation were performed in Python, and a web-based interface was developed to display detection outputs. Results show that the lightweight IDS achieved 80.61% accuracy, a very small model size of 26.33 KB, and a low detection latency of 0.533 ms-making it suitable for IoT edge deployment. Although traditional models achieved higher accuracies, their computational and memory demands make them unsuitable for constrained devices. The study concludes that lightweight AI-driven IDS solutions can effectively balance accuracy and resource efficiency, making them ideal for IoT environments such as smart homes, healthcare, and industrial applications.

Keywords: *Intrusion Detection System, IoT Networks, Lightweight Machine Learning*

1. Introduction

The Internet of Things (IoT) represents one of the most significant technology revolutions of the 21st century, connecting billions of devices across households, industries, healthcare, transportation, and urban infrastructure. Automation, efficiency, and intelligent decision-making are made possible by these devices' real-time data collection, processing, and transmission capabilities [1]. IoT has become an essential part of contemporary life, enabling
cutting-edge ideas like Industry 4.0 and smart cities, from wearable health monitors and smart thermostats to industrial robots and driverless cars [2] projected that by 2030, there will be more than 25 billion IoT-connected devices globally, indicating the technology's quick uptake. Both the potential advantages of IoT systems and the related security issues are highlighted by this exponential expansion.

Despite its benefits, IoT's operational and architectural constraints make it intrinsically susceptible to cyber-attacks. IoT devices, in contrast to traditional computer platforms, frequently have limited battery life, memory, and processing capability. The implementation of traditional security measures like firewalls, antivirus programs, and computationally demanding deep learning-based IDSs is hampered by these constraints [2]. IoT devices are therefore a desirable target for cybercriminals who take advantage of these flaws for nefarious ends. Recent events, such as the widespread Mirai botnet assaults, have shown how thousands of IoT devices with inadequate security can be taken over at the same time to launch enormous distributed denial-of-service (DDoS) attacks that severely disrupt internet services [3]. IoT networks are increasingly vulnerable to man-in-the-middle attacks, spoofing, unauthorized data exfiltration, and zero-day vulnerabilities in addition to DDoS, all of which present serious hazards to people, companies, and vital infrastructure [4].

IDS have been frequently suggested as a security mechanism for monitoring IoT traffic and identifying unusual or malicious activity in order to reduce these dangers. Signature-based and anomaly-based detection are the two main types of IDS solutions. Because signature-based IDS rely on established harmful behavior patterns, they are good at spotting known assaults but useless against emerging or novel threats. In contrast, anomaly-based IDS detect unknown or zero-day assaults by focusing on identifying deviations from typical traffic behavior. However, anomaly-based approaches are less useful in resource-constrained IoT systems since they

frequently demand higher computational resources and are prone to producing false positives [5]. As a result, even while IDS is still a vital tool for IoT security, current methods find it difficult to strike the practical balance between accuracy, efficiency, and scalability.

Machine learning (ML) and artificial intelligence (AI) have created new opportunities to overcome these constraints. ML algorithms are especially well suited for dynamic IoT contexts because they can learn traffic patterns from data and adapt to changing risks, unlike classic rule-based systems. Because of their comparatively low computational cost and efficiency when compared to deep learning models, lightweight machine learning algorithms like Decision Trees, Logistic Regression, Naïve Bayes, and Isolation Forest have become promising candidates for IoT intrusion detection [4]. Among these, Isolation Forest has drawn interest due to its capacity for anomaly identification and effectiveness in managing large-scale, high-dimensional data without requiring a lot of memory or processing power [2]. This makes it especially appropriate for IoT systems, where dependable detection is essential but resources are limited.

The availability of high-quality, publicly accessible IoT datasets has improved researchers' capacity to train and assess IDS models in real-world scenarios in addition to algorithmic advancements. Intrusion detection techniques can be thoroughly tested across a variety of IoT-specific threat vectors thanks to datasets like Bot-IoT [6], IoT-23 [7], and the recently released CICIoT2023 dataset [8]. These datasets enable researchers to validate IDS performance on real-world-like data, going beyond small-scale laboratory studies.

However, there are still issues with making sure that IoT IDS systems minimize latency, save energy, and lower computational overhead in addition to achieving high detection accuracy. Many current methods still place a strong emphasis on accuracy as the main evaluation parameter, ignoring other important aspects like efficiency and scalability in settings with limited resources [9]. By developing and testing an AI-enhanced IDS based on Isolation Forest in simulated IoT environments, this study aims to close these gaps. The study intends to provide a useful and resource-conscious paradigm for improving IoT security in the face of changing cyber threats by concentrating on striking a balance between accuracy, latency, and energy efficiency

1.1 Related Works

Fenanir, *et al.* [10] proposes a lightweight IDS for the IoT that combines multiple machine learning classifiers with filter-based feature selection. Logistic regression, naïve Bayes, decision tree, random forest, KNN, SVM, and MLP were compared on three datasets (KDD99, NSL-KDD, and UNSW-NB15), and decision tree was chosen due to its efficiency and accuracy. According to experiments, the IDS is appropriate for IoT contexts with limited resources since it retains good detection performance when characteristics are reduced using correlation techniques.

Berhili, *et al.* [11] reviews how machine learning enhances IDS for IoT)environments. The paper analyze different ML approaches including supervised, unsupervised, and hybrid methods and evaluate their effectiveness in detecting evolving and unknown attacks. They highlight the benefits of ML for improving detection accuracy, reducing false positives, and adapting to diverse IoT traffic. The review also discusses the most common datasets used for IDS research, and identifies open challenges and future research directions for securing IoT using ML-based IDS.

Alashjaee and Alqahtani [12] proposed a hybrid IDS for IoT networks that combines XGBoost with a feed-forward neural network (FFNN). They use PCA for feature selection, preprocess data from the CIC IoT 2023 dataset, and use over- and under sampling to reduce class imbalance. Deep features are extracted by the FFNN and subsequently categorized using XGBoost. Their model outperforms solo FFNN and XGBoost, achieving ~99% accuracy with great precision, recall, and F1-score. For practical IoT implementations, the design is effective and scalable.

Yunusa, *et al.* [13] investigate how adversarial examples generated by a Conditional Tabular GAN (CTGAN) can undermine an LSTM-based IDS. They train a deep LSTM classifier on the NSL-KDD dataset, achieving high performance (accuracy ≈ 0.9607, precision 0.8725, F1 score 0.9210). Then, they use CTGAN to generate adversarial network traffic data that mimics attacks, and test how easily the LSTM model is fooled. The adversarial samples cause the model to misclassify attacks as normal, degrading its accuracy to around 0.5257, with a precision of 0.5656, recall of 1.0, and F1 score of 0.4099. This demonstrates a significant vulnerability in LSTM-based IDS systems and highlights the risk posed by GAN-based adversarial attacks.

Misrak and Melaku [14] proposes a low-power intrusion detection solution designed for IoT devices with limited resources. To reduce input dimensionality, the authors combine advanced feature engineering (RAL-MIFS + two-stage IPCA) with a hybrid DNN–BiLSTM deep learning model. To reduce the model size without sacrificing accuracy, they additionally use Optuna-based hyper parameter adjustment and dynamic quantization (quantization-aware training + post-training quantization). The quantized model, which was only about 25–31kb in size, obtained 99.73% and 93.95% detection accuracy when tested on the CIC-IDS2017 and CIC-IoT2023 datasets. Ismail, *et al.* [15] Uses Three IoT/IIoT datasets (TON_IoT, WUSTL-IIoT-2021, EdgeIIoTset) are used in the study to assess lightweight supervised machine-learning models (Decision Tree, Random Forest, Bagging, Stacking, and LightGBM). They quantify models by precision, recall, micro-F1, size, and training duration, utilize mutual information for feature selection, and examine the effects of unequal class distributions. Additionally, they show real-time deployment performance in a live network and evaluate cross-dataset generalization (training on TON_IoT, testing on WUSTL-IIoT-2021).

Pant, *et al.* [16] Research suggests an AI-enhanced, lightweight IDS for Wireless Body Area Networks (WBANs). It combines an on-node filter with an energy-consumption and physiological feature-based centralized unsupervised convolutional autoencoder (CAE). Reconstruction error from the CAE is used in place of set

criteria to identify abnormalities, including denial-of-sleep and other zero-day attacks. With an F1-score of 0.96 and an AUC of 0.98, the system performs exceptionally well when evaluated on benchmark data and simulated incursions, making it suitable for medical IoT with limited resources.

Wisanwanichthan and Thammawichai [17] Uses knowledge distillation to offer a lightweight IDS for low-power IoT devices and UAVs. A considerably smaller "student" model is trained using a big deep neural network (the "teacher"), transferring knowledge to lower memory and processing requirements. The distilled student model achieves over 90% parameter reduction, 7–11% faster inference, and improved detection metrics (accuracy, F1, AUC) across several benchmark datasets (NSL-KDD, UNSW-NB15, CIC-IDS2017, IoTID20, UAV IDS), making it appropriate for edge deployment. Almotairi, *et al.* [18] suggest a machine-learning IDS for IoT networks that integrates ensemble learning and feature selection. They reduce dimensionality and increase efficiency by choosing the top 15 most important features using the K-Best algorithm. A heterogeneous stack-ensemble classifier made up of conventional machine learning models receives these features. Their ensemble technique performs much better than individual models on the ToN-IoT dataset in terms of accuracy, precision, recall, and F1-score, providing a reliable way to improve IoT security.

Alve and Mahmud [19] Recommends a lightweight ensemble machine-learning framework for identifying and categorizing various assaults on IoT networks. The authors methodically assessed classifiers such as Decision Tree, Random Forest, and others using the CICIoT 2023 dataset (34 attack types across 10 categories). While Random Forest obtained 98.22% accuracy, their Decision Tree model attained 99.56% accuracy and a 99.62% F1 score. By balancing high detection performance with low computational overhead, the work demonstrates that straightforward, resource-efficient machine learning models can consistently safeguard IoT devices.

1.2 Background

IDS have emerged as a key component of contemporary IoT cyber security, acting as proactive mechanisms to monitor traffic and system activities and identify potentially malicious behaviors before they escalate into large-scale compromises [20]. In contrast to traditional IDS solutions deployed in enterprise or cloud environments with ample computing resources, IDS for the IoT [3]. These limitations make the direct adoption of resource-intensive detection techniques. Massive amounts of heterogeneous data are produced by their interconnection, which makes automation, efficiency, and predictive intelligence possible. IoT devices are expected to surpass 25 billion globally by 2030, according to[21], highlighting their rapid uptake. However, IoT ecosystems are now very appealing to cybercriminals due to their scale and heterogeneity, which have also increased the attack surface.

Unfortunately, security is frequently overlooked in favor of economy and usability when designing IoT devices. They are vulnerable to a range of cyber-attacks, including denial of service (DoS), distributed denial of service (DDoS), spoofing, virus propagation, and data exfiltration, due to their restricted processing power, shoddy authentication procedures, and dependence on out-of-date or unpatched firmware. Poorly secured IoT devices were used in the infamous Mirai botnet assault in 2016 to conduct one of the biggest known DDoS operations, severely impairing major internet services worldwide [22]. Malware families like Mozi and Gafgyt have developed recently to take advantage of unencrypted communication and lax authentication in IoT systems, maintaining a constant threat landscape [23].

As a result, IDS has gained widespread recognition as an additional line of protection to conventional preventive controls. IDS methods can be broadly divided into two paradigms: anomaly-based detection and signature-based detection. Because they rely on pre-established rules, signature-based systems which are used in programs like Snort or Suricata are very good at identifying known threats with few false positives, but they are vulnerable to zero-day attacks [9]. Anomaly-based systems, on the other hand, use machine learning (ML) and artificial intelligence (AI) to learn typical traffic patterns and identify variations that might indicate intrusions. In resource-constrained IoT environments, this paradigm frequently experiences high false positive rates and substantial computational demands, despite being more adaptable and resistant to new threats [20].

These issues have been addressed by recent developments in lightweight machine learning models. For real-time IoT intrusion detection, algorithms like Decision Trees (DT), Naïve Bayes (NB), Logistic Regression (LR), K-Nearest Neighbors (KNN), and Isolation Forest (IF) have proven to be able to strike a balance between efficiency and detection accuracy [9]; [4]. Lightweight models are better suited for energy-constrained IoT deployments than deep learning techniques, which yield excellent accuracy but need substantial computing and memory resources. Recent benchmark datasets as Edge-IIoTset (2022), IoT-23, and CICIoT2023 have made it possible to evaluate IDS techniques in IoT-specific situations in a consistent and repeatable manner, which has advanced this research [20]. Despite extensive research on IDS for the IoT, real-world deployment remains difficult because many solutions rely on computationally intensive deep learning models that exceed the processing, memory, and energy limits of typical IoT devices [12]. Existing studies often emphasize accuracy alone while neglecting critical operational factors such as latency, energy consumption, and resource footprint metrics essential for battery powered and resource-constrained environments [24]. Moreover, several IDS solutions provide limited attack coverage, focusing mainly on DoS/DDoS while overlooking threats like spoofing, reconnaissance, data exfiltration, and botnet activity [25]. A further limitation is the dependence on offline datasets without validation on realistic edge platforms, raising concerns about generalizability and real-time performance. These gaps underscore the need for lightweight, resource-efficient IDS capable of handling diverse attack types and suitable for deployment on constrained IoT hardware. To design and implement an AI-enhanced lightweight intrusion detection system for IoT networks, optimized for detecting cyber threats in resource-

limited environments, we propose IDS tailored for IoT using lightweight machine learning algorithms to:

a. Develop the proposed IDS for real-time IoT threat detection.
b. Evaluate the anomaly-based performance of the IDS.
c. Compare the system against existing IDS approaches in simulated IoT environments.

2. Evaluation Methods

The suggested methods, which include data collection, pre-processing, feature selection, choosing suitable classification models, training and testing the models, performance evaluation, and implementation, are the primary subject matter of this section.

An organized approach that combines system analysis with systematic design principles is necessary for the creation of efficient IDS for IoT environments. Given the particular limitations of the IoT, namely its limited memory, computing capacity, and energy. This study uses a hybrid approach that incorporates aspects of both Rapid Application Development (RAD) and the Waterfall model. While RAD introduces iterative prototyping to refine components like data preprocessing, model selection, and system validation in response to empirical results, the Waterfall model guarantees that the system follows a clear sequential process from requirements gathering to testing and evaluation [9]. This combination strikes a balance between the flexibility needed in applied machine learning research and methodological rigor. The adapted methodology consists of six interconnected stages:

a. Problem Definition and Requirement Analysis: In this phase, the security requirements of IoT systems were determined by evaluating the literature, comparing the limitations of the present IDS, and establishing the system's goals. With a focus on lightweight processing, scalability, and flexibility to changing attack patterns, the outputs comprise the functional and non-functional requirements of the suggested IDS [24].
b. System Modeling and Conceptual Design: At this point, entity-relationship diagrams (ERDs), data flow diagrams (DFDs), and conceptual frameworks are used to establish the logical structure of the system. Prior to implementation, this modeling stage makes sure that user interactions and data channels (traffic collecting, preprocessing, detection, and alerting) are clearly defined [20].
c. Dataset Acquisition and Preprocessing: Public benchmark datasets like IoT-23, CICIoT2023, and TON_IoT were used. To ensure consistency and comparability with previous efforts, preprocessing approaches such as feature selection, category encoding, and normalization are used to prepare data for lightweight model training.
d. Model Development and Algorithm Selection: Throughout the implementation and testing, lightweight machine learning models including Isolation Forest, Decision Trees, and Random Forest were employed. To reduce memory and computational load while optimizing detection performance, model optimization techniques like feature reduction and hyper parameter tweaking were used.
e. System Architecture and Prototype Implementation: A modular architecture comprising input (traffic data), preprocessing, detection engine, and alarm generation modules was used to construct the IDS. Python (Scikit-learn, pandas, NumPy) and visualization tools were used to put up a simulation environment. The architecture is designed to be deployed on IoT nodes with little resources.
f. Evaluation and Validation: Metrics for detection performance (accuracy, precision, recall, F1-score, ROC-AUC), operational efficiency (latency, throughput, memory footprint), and resource consumption (energy consumption, false alarm rate) was used to test the system. To assess generalization and resistance to new traffic patterns, cross-dataset validation was used.

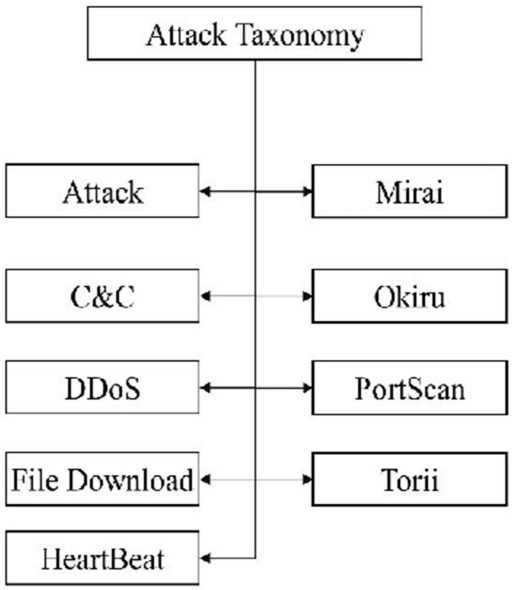

Figure 1: IoT-23-Dataset-attack-taxonomy-B-feature-processing [5]

2.1 Anomaly-based IDS in IoT

Using statistical or machine learning techniques, anomaly-based IDS identify departures from predetermined "normal" behavior profiles [17]. These solutions are more suited to the dynamic and unpredictable nature of IoT environments since they can identify new intrusions and zero-day assaults. For instance, [26] created N-BaIoT, a deep autoencoder-based anomaly-based intrusion detection system that effectively detected IoT botnet attacks. However, AIDS faces difficulties such high false positive rates if typical behavior is poorly described and the computational demands of machine learning methods, which may be too much for devices with limited resources.

2.2 Lightweight machine learning models

The capacity of IDS to identify both established and new cyber threats has been greatly enhanced by the incorporation of machine learning. However, because to

their high memory, processing power, and energy requirements, deep learning techniques like convolutional neural networks (CNNs) and recurrent neural networks (RNNs) remain unfeasible for the majority of IoT applications [27]. On the other hand, lightweight machine learning models are becoming more and more popular as a potential remedy. These models are appropriate for deployment on IoT devices with limited hardware because they are made to balance computational economy and detection accuracy.

While maintaining competitive performance against sophisticated assaults, lightweight models prioritize quicker training cycles, lower memory usage, and low inference latency. According to recent research, correctly designed lightweight models can even perform better than heavier deep learning architectures in resource-constrained IoT environments, especially when explainability and real-time responsiveness (RTR) are crucial [28].

2.3 Tree-based models

Among the most popular lightweight models in IoT IDS are tree-based algorithms like Decision Trees (DT), Random Forests (RF), and Gradient Boosting frameworks e.g., LightGBM, XGBoost. Their interpretability, low computing cost, and quick training are what make them appealing [29]. According to recent assessments, RF and LightGBM can achieve accuracy levels that are on par with deep neural networks while still being practical for use on edge devices and IoT gateways [30].

2.4 Probabilistic models

For lightweight IDS in IoT, probabilistic classifiers like Naïve Bayes (NB) and Logistic Regression (LR) continue to be excellent options. When it comes to category or binary attack categorization tasks, these models work especially well. It has been demonstrated that NB is straightforward but effective, offering good adaptability for anomaly-based IDS with low computing resource requirements [31].

2.5 Instance-based and neural models

Although K-Nearest Neighbors (KNN) and other instance-based techniques can achieve excellent detection accuracy, their processing demands do not scale well with bigger datasets. To make the algorithm more useful for small- to medium-sized IoT networks, optimized or approximate KNN variations have been proposed [32].

For lightweight IDS, shallow neural architectures like autoencoders and basic Multi-Layer Perceptrons (MLPs) have been modified. For example, the Kitsune framework shows that even on limited devices, ensembles of tiny autoencoders can identify abnormalities in real time [33]. By combining lightweight autoencoders with federated learning, more recent research expands on this and enhances scalability and data privacy in IoT deployments [34].

2.6 Model optimization techniques

Optimization techniques are essential for effectively implementing machine learning models because of IoT's stringent resource constraints:

a. Quantization: Significantly reduces memory and compute requirements by reducing numerical precision (e.g., from 32-bit to 8-bit) [35].
b. Pruning: Makes models smaller and faster by removing unnecessary model parameters (Han et al., 2016).
c. Knowledge distillation: Transfers knowledge from a big, intricate "teacher" model to a smaller "student" model without significantly lowering performance [36].
d. These optimization techniques guarantee that IDS models maintain their energy and memory efficiency while achieving excellent accuracy, which is essential for realistic IoT implementation.

2.7 Evaluation metrics

The study will use an extensive method of evaluation to persuasively show the security efficacy and feasibility of the suggested IDS for IoT. The evaluation will focus on three main areas: resource/energy consumption, operating efficiency, and detection performance, based on findings from recent literature [20].

2.7.1 Detection performance (security metrics)

The accuracy with which the IDS detect harmful activity is the first dimension. Standard metrics will be supplied, including ROC-AUC, F1-score, recall (or detection rate), accuracy, and precision. Although accuracy indicates general correctness, it might be deceptive when attack classes are few. Recall measures the percentage of real attacks that were successfully identified, whereas precision measures the percentage of warnings that match actual threats. Both are balanced by their harmonic mean, the F1-score, which is especially crucial for IoT traffic, which is frequently unbalanced. In order to ensure that minority but high-impact risks like spoofing or exfiltration are not missed, studies using datasets like IoT-23 and CICIoT2023 emphasize the importance of reporting per-class precision and recall as well as both macro- and micro-averaged F1 [20]. ROC-AUC will highlight trade-offs between sensitivity and specificity and also demonstrate classifier resilience across decision thresholds [32]

The accuracy with which the IDS detect malicious activity will be evaluated using these metrics:

a. Accuracy: Calculates the total percentage of instances both benign and malevolent that are accurately classified. However, with unbalanced datasets, accuracy alone may be deceptive and the expression for this evaluation metric is in equation 1:

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

b. Precision: shows the proportion of attacks that have been reported as being actually malicious. Fewer false alarms result from high precision. Precision is a significant metric. It is expressed as in equation 2:

$$PC = \frac{TP}{TP+FP} \quad (2)$$

c. Recall (Detection Rate): Calculates the proportion of real attacks that are accurately detected.
d. A high recall guarantees fewer hazards are overlooked and it is written as in equation 3:

$$RC = \frac{TP}{TP+FN} \quad (3)$$

e. F1-Score: A balanced measure of both precision and recall, calculated as the harmonic mean of the two. It is evaluated by equation 4:

$$F_1 - Score = 2 * \frac{Precision*Recall}{Precision+Recall} \quad (4)$$

2.7.2 Operational efficiency (real-time responsiveness)

Accurate detection is not sufficient in IoT installations; the IDS must also function swiftly and seamlessly on limited devices. Thus, measurements like inference latency (time per packet/flow), throughput (flows processed per second), and memory footprint will be used to assess the system. These metrics show whether the solution can actually operate on IoT gateways with restricted resources. Previous research highlights that even "lightweight" models may fail if they are unable to process traffic at line speed or if memory usage surpasses device capacity [21]. Performance will be evaluated on practical edge devices like Raspberry Pi or ARM-based boards to guarantee relevance.

2.7.3 Resource and energy consumption

Energy efficiency is another important factor. Energy draw will be monitored directly wherever feasible (e.g., joules per inference). Estimates will be based on inference time and CPU utilization in cases where hardware does not enable this. Since model size affects storage, transmission overhead, and startup time, it will also be reported. Since needless warnings result in extra processing, logging, and communication that consume bandwidth and power, the false positive rate will be considered both a detection and resource cost. According to earlier research, assessing energy in addition to accuracy gives a more accurate picture of IDS appropriateness, especially for industrial IoT [37].

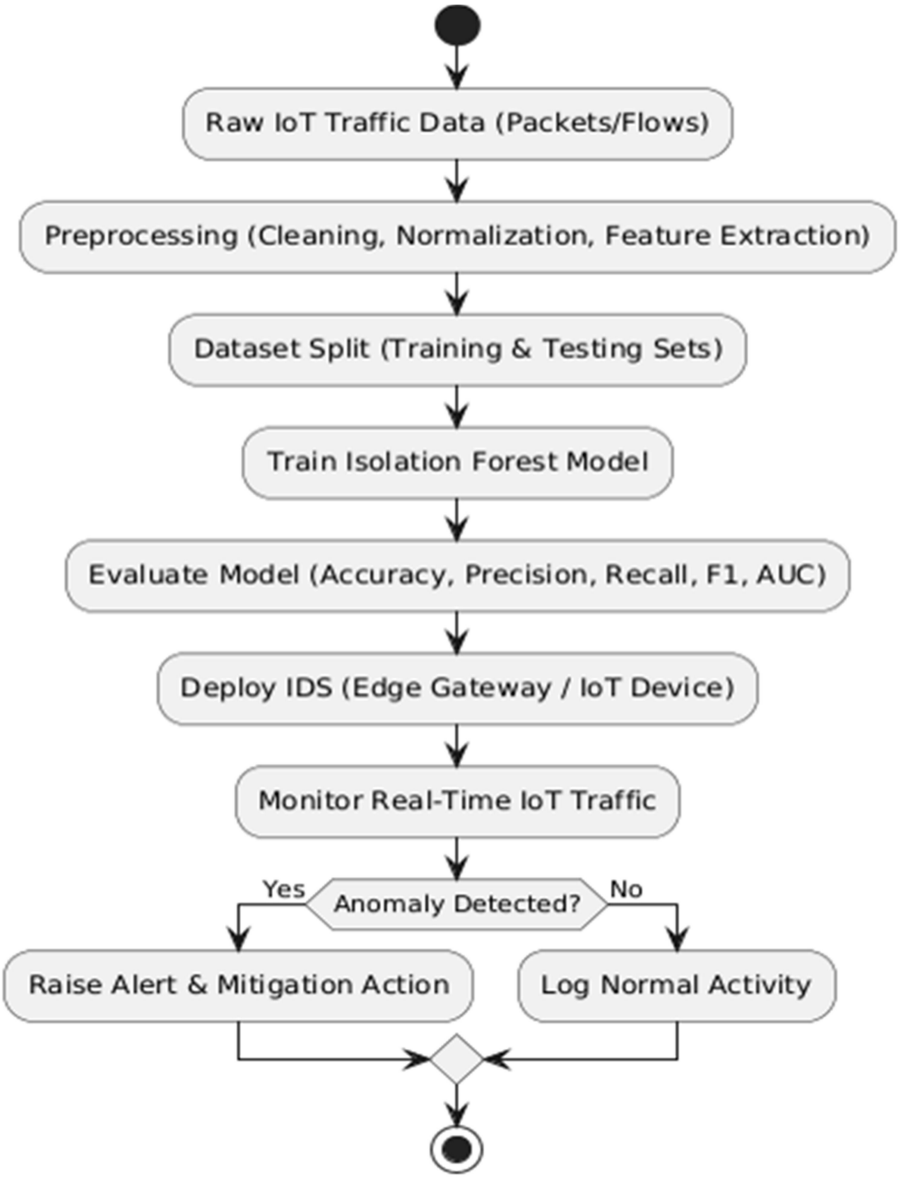

Figure 2: System Vertical Workflow diagram

Generalization across datasets: Lastly, cross-dataset assessments will be used to test resilience. For instance, models developed on IoT-23 might be verified against TON_IoT or CICIoT2023. Research frequently cautions that while cross-dataset validation reveals generalization limits and more closely resembles deployment in real-world settings, single-dataset tests may overstate performance [8, 20]. This guarantees that the suggested IDS is durable in a variety of unforeseen traffic scenarios and is not over fitted to lab-specific conditions.

2.8 Lightweight machine learning models for anomaly detection

The constraints of current systems, especially those pertaining to scalability, resource consumption, and detection accuracy, have been carefully considered in the design of the proposed IDS for IoT networks. The system incorporates lightweight machine learning models for anomaly identification in order to accomplish this, with an emphasis on the Isolation Forest algorithm because of its effectiveness in identifying outliers with low computing cost [38].

Additionally, alternative lightweight models like Naïve Bayes, Random Forests, and Decision Trees will be taken into consideration for comparative benchmarking. This guarantees that the IDS not only shows how successful Isolation Forest is, but also offers information on how it compares to other strategies.

The design is organized around conceptual models, architectural specifications, theoretical underpinnings, and a guiding framework that connects the system's practical execution with the goals of the study. The following subsections provide descriptions of these design components.

2.9 Dataset description

The study uses benchmark and current IoT datasets, like: The CICIoT2023 Dataset This dataset was created by the Canadian Institute for Cybersecurity and includes both benign traffic flows and a variety of contemporary IoT attack scenarios, such as botnet traffic, data exfiltration, and distributed denial of service (DDoS). For IoT IDS research, it is regarded as one of the most recent and extensive datasets.

IoT-23 Dataset was made available by Stratosphere IPS, includes three benign and twenty distinct malware captures from actual IoT devices. It is appropriate for anomaly-based detection investigations because it includes a variety of attack families, such as Gafgyt and Mirai and BoT-IoT.

Dataset which was developed by the Australian Centre for Cyber Security, this dataset mimics the actions of IoT botnets and records attacks including data theft, DoS, and DDoS. Because it is labeled and structured, it is quite common in IDS benchmarking. The datasets exhibits the following set of attributes:

a. Traffic Type: Consists of flow-based and packet-level data from IoT devices.
b. Labels: Every traffic instance is categorized as either benign or belonging to one of numerous categories of harmful attacks.
c. Features: There are attributes like source/destination IP, packet length, protocol type, flow time, and connection state. Both statistical and behavioral analyses of network traffic are made possible by these qualities.

Attack Diversity: A variety of attack vectors, including as DDoS, spoofing, botnets, and exfiltration, are included in the datasets, guaranteeing that the IDS is assessed in a variety of threat scenarios.

3. Results and Discussion

The intuitive web interface that allows for the uploading of datasets, the execution of detection, and the visualization of metrics was implemented. Table 1 demonstrates the system's operational viability

Table 1: Main Features of the Implemented Lightweight IDS System

.Feature	Description
Dataset Upload	Users can upload IoT traffic data for evaluation.
Detection Execution	Runs the proposed IDS model on the uploaded dataset.
Results Visualization	Displays detection metrics (Accuracy, Precision, Recall, F1, FPR, ROC AUC).
Efficiency Metrics	Shows model size, latency, and training time for the uploaded dataset.
Comparative Analysis	Provides side-by-side comparison with Decision Tree and Random Forest.

3.1 Anomaly-based IDS

The performance of the Intrusion Detection System was evaluated using anomaly-based detection metrics, including: Accuracy, Precision, Recall, F1-Score, False Positive Rate (FPR) and ROC AUC. A classification model's performance metrics are shown in Table 2. With an accuracy of 80.61%, the model accurately classifies the majority of inputs. Its recall of 80.61% demonstrates its great ability to identify real positive instances, while its precision of 79.96% indicates that most predicted positive cases are actually positive.

Table 2: Detection Performance Metrics of the Proposed Lightweight IDS on IoT Datasets

Metric	Value (%)
Accuracy	80.61
Precision	79.96
Recall	80.61
F1-score	75.38
False Positive Rate	47.69
ROC AUC	0.893

Despite being somewhat lower because of performance trade-offs, the F1-score of 75.38% is a balanced indicator of precision and recall. The model frequently misclassifies typical cases as assaults, as indicated by the comparatively high false positive rate (FPR) of 47.69%. Despite this, the model performs well

over a range of classification thresholds, as evidenced by the ROC AUC value of 0.893, which demonstrates high overall discrimination ability between classes.

3.2 Efficiency comparison

Efficiency metrics assess resource consumption, which is critical for IoT deployment. A comparison between these three IDS models was done as shown in Table 3, including: Random Forest, Decision Tree, and Isolation Forest. Where: the Random Forest is by far the largest model (≈654 MB), resulting in the highest latency (10.66ms) and the longest training time (466.42s), while the Decision Tree is larger (2,558.82kb) but achieves the lowest latency (0.148ms), responding faster than the others despite a moderate training time of 28.55s). This indicates that while Random Forest can deliver strong accuracy in many tasks, it is computationally expensive and inefficient for latency-sensitive or resource-constrained IDS environments. A graphical representation n of the result is displayed in Figure 3

Table 3: Model Size and Inference Latency Comparison of Lightweight and Conventional IDS Models

IDS Model	Model Size (kb)	Median Latency (ms)	Training Time (s)
Isolation Forest	26.33	0.533	20.55
Decision Tree	2,558.82	0.148	28.19
Random Forest	654,759.54	10.66	466.42

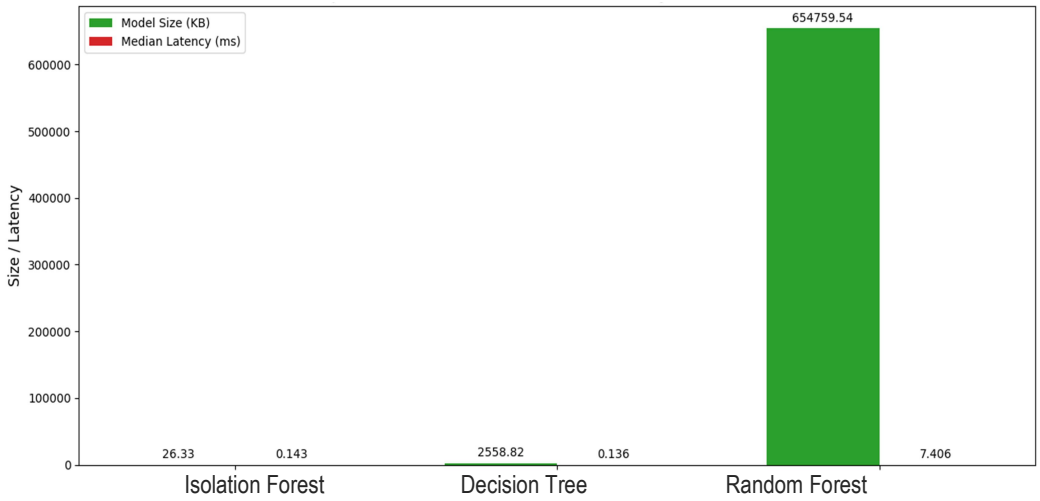

Figure 3: Bar chart comparing model size and latency across models

3.3 Efficiency metrics

Overall, these metrics highlight a compact, responsive, and computationally efficient model. The model's median inference latency of 0.533ms indicates extremely fast prediction time, enabling near real-time decision-making; its training time of 20.55 seconds shows that it can be trained quickly, reducing computational cost and allowing rapid iterations or retraining when necessary; and its size of only 26.33kb requires minimal storage, making it highly suitable for deployment on resource-constrained devices.

Table 4: Model size, latency, and training time of the proposed IoT-Compatible IDS

Metric	Value
Model Size (KB)	26.33
Median Inference Latency (ms)	0.533
Training Time (s)	20.55

The IDS was compared against Decision Tree and Random Forest, which represent established machine learning approaches for IoT intrusion detection and the result is shown in Table 5 and a graphical representation in Figure 4: The findings demonstrate a notable performance difference between the two tree-based supervised models (Random Forest and Decision Tree) and the Isolation Forest. With an accuracy and recall of 80.61%, the unsupervised anomaly-detection method Isolation Forest performs mediocrely. However, its high false positive rate (47.69%) suggests that it regularly misclassifies regular traffic as assaults, which lowers its overall dependability. Its ROC AUC of 0.893 indicates a respectable but constrained capacity for discrimination.

The Decision Tree model, on the other hand, has a very low false positive rate (0.02%), a high ROC AUC (0.996), and above 99% accuracy, precision, recall, and F1-score. This implies a very accurate and consistent classification. Despite having a comparatively higher false positive rate (11.78%), the Random Forest model performs somewhat better than the Decision Tree in terms of accuracy (99.33%) and ROC AUC (0.997). Because of its ensemble structure, it has great detection capabilities and is robust. All things considered, tree-based supervised models perform significantly better than the unsupervised Isolation Forest, with Random Forest providing the best overall discrimination even if it's FPR is greater.

Table 5: Detection performance comparison in accuracy and precision

IDS Model	Accuracy (%)	Precision (%)	Recall (%)	F1 (%)	FPR (%)	ROC AUC
Isolation Forest	80.61	79.96	80.61	75.38	47.69	0.893
Decision Tree	99.28	99.29	99.28	99.28	0.02	0.996
Random Forest	99.33	99.31	99.33	99.28	11.78	0.997

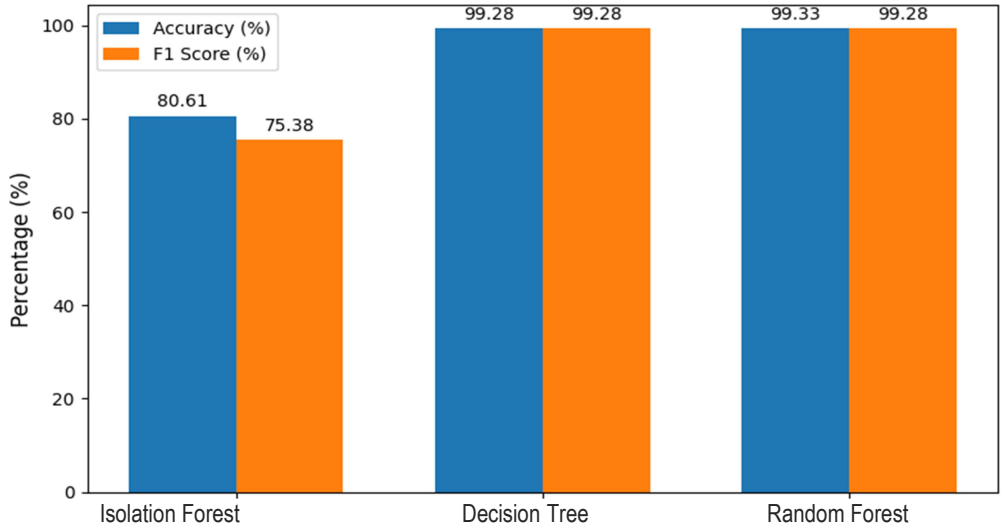

Figure 4: Comparison of Accuracy and F1-Score between Decision Tree, Random Forest and the Isolation Forest Models

4. Conclusion

The study effectively showed that, even in settings with limited resources, it is feasible to design, implement, and assess lightweight AI-enhanced IDS that can effectively identify anomalies within IoT networks. The system addressed one of the most important issues in IoT cyber security limited device resources by striking a balance between detection accuracy, computational economy, and scalability through the deployment of optimized lightweight machine learning techniques. The experimental findings verify that the suggested IDS maintains a small model size and low processing latency while providing robust detection capabilities with acceptable accuracy, precision, and F1-Scores. This shows that large computational models, which are frequently prohibitive for IoT edge devices, are not necessary to achieve successful intrusion detection. The results also show that the proposed IDS offer an ideal trade-off between resource consumption and detection performance, which is essential for real-time network security in embedded and dispersed IoT systems.

These results were further reinforced by a comparison with traditional models like Random Forest and Decision Tree. The Random Forest classifier was less appropriate for real-time or edge-based deployments because of its much bigger model size and longer inference time, despite its higher detection accuracy. On the other hand, despite having somewhat lower accuracy, the lightweight IDS was far more effective in terms of memory usage and processing speed, confirming its appropriateness for IoT contexts with constrained computational power, bandwidth, and energy. The report also emphasizes how crucial context-aware system design is to IoT cyber security. This study shows that while developing IDS solutions for IoT applications, system designers should take deployment restrictions, adaptability, and sustainability into account rather than just accuracy. This attitude is supported by the lightweight IDS model created here, which allows for real-time detection and flexibility without sacrificing performance effectiveness.

Recommendations

The following suggestions are put out in light of the findings:

a. Deployment on Real Devices: To verify the IDS's functionality under real-world circumstances, future research should include deploying it on real IoT devices.
b. Hybrid or Ensemble Models: Using ensemble techniques or hybrid lightweight models could increase detection accuracy without appreciably consuming more resources.
c. Constant Dataset Updates: In order to adjust to changing attack tactics, the IDS should be retrained on a regular basis using new IoT traffic datasets.
d. Improved online Interface: Upcoming improvements to the online interface may include alert notifications for serious threats and visualization dashboards for real-time monitoring.
e. Security Integration: Network security may be strengthened even more by integrating with additional IoT security measures like intrusion prevention systems or firewalls

References

[1]. Dubey, K., Dubey, R., Panedy, S. and Kumar, S., (2014). A review of iot security: machine learning and deep learning perspective, *Procedia Computer Science.* 235, 335–346.

[2]. Wang, M., Sun, Y., Sun, H. and Zhang, B., (2023). Security issues on industrial internet of things : Overview and challenges, *Computers*, vol. 12, no. 12, 1-27.

[3]. Hafiz, G., Ahmad, U., Iqra, Y., Muhammad, A., Tehseen, M., Muhammad, A.K., Ines, H.J. and Habib, H., (2025). Energy-efficient deep learning-based intrusion detection system for edge computing: a novel DNN-KDQ model, *Journal of Cloud Computing*, 14, Art. no. 32, 1-27.

[4]. Jonathan, L., Anel, H., Torstein, M. K., Håkon, P., Jacob, H., Magnus, H. J. and Moritz, P. N. H., (2025). Lightweight machine learning models for intrusion detection on IoT Devices, *Nor. IKT-konferanse Forsk. og utdanning*, 37(3), 1-21 https://doi.org/10.5324/jrxdjb92.

[5]. Ullah, I. and Mahmoud, Q., (2021). Design and development of a deep learning-based model for anomaly detection in IoT networks, *IEEE Access*, PP, 9, 103906–103926. https://doi.org/10.1109/ACCESS.2021.3094024.

[6]. Koroniotis, N., Moustafa, N., Sitnikova, E. and Turnbull, B., (2019). Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset, *Future Generation Computer Systems*, 100, 779–796,

[7]. García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G. and Vázquez, E., (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges, *Computers and Security,* 28(1), 18–28.

[8]. Alex, C., Creado, G., Almobaideen, W., Alghanam, O. A. and Saadeh, M., (2023). A comprehensive survey for iot security datasets taxonomy, classification and machine learning mechanisms, *Computers and Security*, 132, 103283.

[9]. Alomari, Z., Li, Z. and Makanju, A., (2024). Lightweight machine learning-based ids for iot environments, in *Proceedings of the 8th Cyber Security in Networking Conference*, Paris, France,

[10]. Fenanir, S., Semchedine, F. and Baadache, A., (2019). A machine learning-based lightweight intrusion detection system for the internet of things, *Revue d'Intelligence Artificielle*, 33, 203–211,

[11] Berhili, M., Chaieb, O. and Benabdellah, M., (2024). Intrusion detection systems in IoT based on machine learning: A state of the art, *Procedia Computer Science*, 251, 99–107.

[12] Alashjaee, A. M. and Alqahtani, F., (2025). Enhanced intrusion detection system IoT network security model by feed forward neural network and machine learning, *Scientific Reports*, *15*(1), 36085.

[13]. Yunusa, A. A., Zambuk, F. U., Ya'u, B. I., Umar, A. and Disina, A. H. (2023). "CTGAN adversarial attack on network intrusion detection based on LSTM algorithm, *ASRIC Journal of Natural Sciences*, 3(1), 182–193.

[14]. Misrak, S. F. and Melaku, H. M., (2025). Lightweight intrusion detection system for IoT with improved feature engineering and advanced dynamic quantization, *Discover Internet of Things*, 5, Art. no. 97,1-34.

[15]. Ismail, S., Dandan, S. and Qushou, A. A, (2025). Intrusion detection in IoT and IIoT: Comparing lightweight machine learning techniques using TON_IoT, WUSTL-IIOT-2021, and EdgeIIoTset Datasets, *IEEE Access*, 13, 73468–73485.

[16]. Pant, D., Lohani, S. and Wason, M., (2025). A lightweight, AI enhanced intrusion detection system for wireless body area networks using unsupervised anomaly detection, *International Journal of Global Innovations and Solutions*, 2(1), 1-10.

[17]. Wisanwanichthan, T. and Thammawichai, M., (2025). A lightweight intrusion detection system for IoT and UAV using deep neural networks with knowledge distillation, *Computers*, 14(7), 1-25.

[18]. Almotairi, A., Atawneh, S., Khashan, O. A., and Khafajah, N. M., (2024). Enhancing intrusion detection in IoT networks using machine learning-based feature selection and ensemble models. *Systems Science and Control Engineering*, *12*(1), 2321381.

[19]. Alve, S. R., Mahmud, M. Z., Islam, S., Chowdhury, M. A., and Islam, J., (2025). *Smart IoT security: Lightweight machine learning techniques for multi-class attack detection in IoT networks*, International Conference on Quantum Photonics, Artificial Intelligence, and Networking (QPAIN) *2025, Rangpur, Bangladesh* 1-6.

[20]. Krzysztoń, E., Rojek, I. and Mikołajewski, D., (2024). A comparative analysis of anomaly detection methods in IoT networks: An experimental study, *Applied Sciences*, 14(24), art. 11545, 1-22,

[21]. I Iacobelli, E., Ponzi, V., Puglisi, A., Kuznetsov, O., Nieszporek, K., Randieri, C. and Napoli, C., (2025). Lightweight anomaly detection for IoT: Evaluating machine learning and deep learning models on CICIDS2017, *International Conference on Artificial Intelligence and Soft Computing* (25-37). Cham: Springer Nature Switzerland.

[22]. Ge, M., Fu, X., Syed, N., Baig, Z., Teo, G. and Robles Kelly, A., (2019). Deep learning based intrusion detection for IoT networks, *in IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC)*, Kyoto, Japan, 256–265,

[23]. Kanin, E., Osiptsov, A., Vainshtein, A. and Burnaev, E., (2019). A predictive model for steady state multiphase pipe flow: Machine learning on lab

data, *Journal of Petroleum Science and Engineering,* 180, 727–746.

[24]. Kuppa, A., Aouad, L. and Le-Khac, N. A., (2021). *Towards improving privacy of synthetic datasets*. 9th Annual Privacy Forum, APF 2021, Oslo, Norway, *Proceedings (Lecture Notes in Computer Science*, 12703), 73–88.

[25]. Hussain, F., Abbas, S. G., Husnain, M., Fayyaz, U. U., Shahzad, F. and Shah, G. A., (2020). IoT DoS and DDoS attack detection using ResNet. In *Proceedings of the 2020 IEEE 23rd International Multitopic Conference (INMIC)*, Bahawalpur, Pakistan, 5 7, 2020, 1–6.

[26]. Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Breitenbacher, D., Shabtai, A. and Elovici, Y., (2018). N-BaIoT-network-based detection of IoT botnet attacks using deep autoencoders, *IEEE Pervasive Computing*, 17(3), 12–22.

[27]. Nguyen, G., Dlugolinsky, S., Bobák, M., Tran, V. D., López G. Á., Heredia I., Malík P. and Hluchý, L., (2019). Machine learning and deep learning frameworks and libraries for large-scale data mining: a survey, *Artificial Intelligence Review*, 52(1), 77–124.

[28]. Alzahrani, O. A. and Alenazi, M. J. F., (2021). Designing a network intrusion detection system based on machine learning for software defined networks, *Future Internet*, 13(5), 111, 1-18,

[29]. Hindy, H., Brosset, D. E., Bayne, A., Seeam, C., Tachtatzis, R. and Bellekens, X., (2018). A taxonomy and survey of intrusion detection system design techniques, *Network Threats and Datasets," CoRR*, vol. abs/1806.03517, 1-35..

[30]. Otoom, A. F., Eleisah, W. and Abdallah, E. E., (2023). Deep learning for accurate detection of brute force attacks on IoT networks, *Procedia Computer Science*, 220, 291–298,

[31]. Ali, H. A. S. and Rani, J. V., (2024). Machine learning for internet of things (IoT) security: A comprehensive survey, *International Journal of Computer Networks and Applications (IJCNA*), 11(5), 617–659.

[32]. Muhammed, A. I., Disina, A. H. Sani, N. M. and Salisu, A. S., (2025). A model for early prediction of chronic kidney disease using machine learning techniques, *Savannah Journal of Science, Engineeering and Technology*, 3(3) 225–232.

[33]. Mirsky, Y., Doitshman, T., Elovici, Y. and Shabtai, A., (2018). Kitsune: An ensemble of autoencoders for online network intrusion detection, *Proceeding of Network and Distributed Systems Security Symposium (NDSS 2018)*, 1-15. San Diego, CA, USA

[34]. Dhakal, R., Raza, W., Tummala, V. and Kandel, L. N., (2024). Enhancing intrusion detection in IoT networks through federated learning, *IEEE Access*, 12, 167168–167182.

[35]. Jacob, B., Kligys, S., Chen, B., Zhu, M., Tang, M., Howard, A., Adam, H., and Kalenichenko, D., (2018). Quantization and training of neural networks for efficient integer-arithmetic-only inference, *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2704–2713.

[36]. Gou, J., Yu B., Maybank, S. J. and Tao, D., (2021). Knowledge distillation: A survey, *International Journal of Computer Vision*, 129(6), 1789–1819.

[37]. Algamdi, H., Aujla, G. S., Singh, A. and Jindal, A., (2025). Energy-aware and explainable automated machine learning for anomaly detection in healthcare IoT, *IEEE Internet of Things Journal*, early access, 12(22), 46215-46224.

[38]. Jamshidi, S., Erfan, F., Abdul-Wahab, O., Bellaiche, M. and Khomh, F., (2025). *lightweight autoencoder-isolation forest anomaly detection for green IoT edge gateways*, *Polytechnique Montr´eal, Quebec, Canada*, 1-23