Intrusion Detection in IoT Environments: An Experimental Evaluation Using Multiple ToN-IoT Dataset Subsets as a Baseline for Federated Learning

RAFAEL SEBASTIÃO GALDINO[1]
CHRISTEL ALEXANDRA HUILCA HINOSTROZA[2]
DEMÓSTENES ZEGARRA RODRÍGUEZ[1]

[1] Department of Computer Science, Federal University of Lavras (UFLA), Lavras, Minas Gerais, Brazil
[2] Universidad Nacional de Ingeniería (UNI), Lima, Peru
raffaelgaldino@gmail.com
christel.huilca.h@uni.pe
demostenes.zegarra@ufla.br

Abstract. The growing adoption of Internet of Things (IoT) devices has increased the need for efficient intrusion detection systems capable of identifying cyberattacks in heterogeneous environments. This work investigates the application of machine learning techniques for intrusion detection using data from the ToN-IoT dataset. Experiments were conducted using Logistic Regression, Random Forest and Multilayer Perceptron (MLP) models applied to different IoT devices, including Weather, Modbus, Garage Door and GPS Tracker. The proposed methodology includes data preprocessing, binary classification of normal and malicious traffic, and comparative evaluation using accuracy, precision, recall and F1-score metrics. The study establishes a reproducible centralized machine learning baseline designed to support the future implementation and evaluation of Federated Learning approaches in IoT environments. Preliminary results demonstrate significant performance differences among the evaluated models, highlighting the importance of model selection for intrusion detection tasks while providing a reproducible experimental baseline for future Federated Learning investigations.

Keywords: Internet of Things, intrusion detection, machine learning, ToN-IoT, federated learning, cybersecurity

(Received May, 2026 / Accepted July, 2026)

1 Introduction

The Internet of Things (IoT) has promoted an increasing integration among connected devices, sensors, embedded systems, and distributed services, enabling applications in areas such as smart cities, healthcare, transportation, industry, and home automation. This broad ecosystem has been supported by advances in intelligent networking, autonomous systems, multimedia services, healthcare technologies, and data-driven applications [11, 18, 31, 49, 52, 53, 56]. The expansion of these connected environments has brought significant advances in automation, monitoring, and real-time communication. However, the growing number of connected devices has also substantially increased the attack surface of networks, making IoT environments frequent targets of cyberattacks, such as Distributed Denial of Service (DDoS), botnets, vulnerability exploitation, and unauthorized access [10, 20, 38, 43–47, 54, 66].

Unlike traditional computing environments, IoT devices often face limitations related to processing power, memory, storage capacity, and energy consumption, making the adoption of conventional security mechanisms particularly challenging. Furthermore, the het-

erogeneity of devices, protocols, and communication standards complicates the implementation of robust monitoring and protection solutions. These constraints are intensified by the growing integration of IoT with software-defined networking, 5G/6G infrastructures, edge services, visible-light communication, and heterogeneous wireless systems [1, 2, 12–14, 19, 21, 35]. In this context, Intrusion Detection Systems (IDS) have received increasing attention as mechanisms capable of identifying malicious behaviors and anomalous activities in real time [38, 43–47, 54, 66].

In recent years, Machine Learning (ML) techniques have played a significant role in the development of intelligent IDS solutions for IoT environments, mainly due to their ability to identify complex patterns and detect previously unknown attacks. Supervised, unsupervised, and deep learning-based approaches have been extensively investigated to improve detection capabilities and reduce false positives in distributed and heterogeneous environments [10, 36, 38, 44, 61, 66]. Recent studies have also highlighted Federated Learning (FL) as a promising alternative for distributed training of detection models without requiring data centralization, contributing to enhanced privacy, scalability, and reduced network traffic in Edge Computing environments [24, 34, 46, 51].

The wider literature also demonstrates that intelligent IoT and communication systems increasingly combine learning-based inference with quality monitoring, sentiment analysis, spatial-data processing, healthcare security, and multimedia services [**?**, 50, 63, 64]. These studies reinforce the broader trend toward data-driven decision making in connected environments, while also emphasizing the importance of privacy, communication efficiency, and dependable operation.

Despite recent advances, important challenges remain regarding the computational cost of models, the resource constraints of IoT devices, and the feasibility of deploying intelligent solutions in edge environments. Moreover, many existing studies focus on complex Deep Learning architectures that require substantial computational resources, limiting their practical applicability in resource-constrained devices [38, 44, 45, 47, 61, 66].

Given this scenario, this work investigates the application of Machine Learning techniques for intrusion detection in IoT environments using subsets of the ToN-IoT dataset. The study evaluates the performance of different supervised classification models, including Logistic Regression, Random Forest, and Multilayer Perceptron (MLP), considering performance metrics widely adopted in the literature, such as Accuracy, Precision, Recall, and F1-Score.

The experiments employ different subsets of the ToN-IoT dataset, including Weather, Modbus, Garage Door, and GPS Tracker devices, enabling the analysis of model behavior across heterogeneous Internet of Things scenarios. The obtained results establish an experimental baseline for future evaluations involving distributed architectures based on Federated Learning.

As a continuation of this research, a federated architecture based on the Federated Averaging (FedAvg) algorithm will be implemented, enabling the investigation of the impact of distributed training on intrusion detection in IoT and Edge Computing environments. In this way, the study seeks to contribute to the development of more efficient, scalable IDS solutions aligned with the privacy requirements of modern Internet of Things ecosystems [24, 34, 46, 51].

The main contributions of this work are: (i) a comparative evaluation of different supervised Machine Learning algorithms applied to intrusion detection across multiple IoT devices from the ToN-IoT dataset; (ii) an analysis of the impact of device-specific characteristics on classifier performance; and (iii) the establishment of an experimental baseline for future Federated Learning-based implementations in distributed IoT environments.

2 Theoretical Background and Related Work

The Internet of Things (IoT) comprises an ecosystem of connected devices capable of continuously collecting, processing, and sharing data over the Internet. Sensors, actuators, cameras, mobile devices, and industrial equipment are integrated into this environment, enabling applications in smart cities, industrial automation, healthcare, agriculture, and intelligent transportation [11, 18, 31, 56]. Despite the benefits associated with connectivity and automation, the expansion of IoT has also significantly increased the attack surface of networks, as devices often exhibit limitations in processing power, storage capacity, and embedded security mechanisms [3, 15, 38, 43–45, 47, 66].

In this context, attacks such as Distributed Denial of Service (DDoS), firmware vulnerability exploitation, botnets, and unauthorized access have become increasingly common in IoT environments. Furthermore, the heterogeneity of devices and communication protocols complicates the implementation of traditional security solutions, making it necessary to adopt intelligent and adaptive mechanisms for network monitoring and protection [25, 55].

2.1 Intrusion Detection Systems in IoT

Intrusion Detection Systems (IDS) are designed to identify suspicious or malicious activities in networks and computing devices, serving as a complement to traditional security mechanisms such as firewalls and access control lists. In general, IDS can be classified into two main approaches: signature-based systems and anomaly-based systems [23, 25].

Signature-based IDS rely on previously known attack patterns to identify malicious activities. Although they provide high accuracy for known threats, they have limitations in detecting novel attacks or previously unseen variants. In contrast, anomaly-based IDS build models of normal network behavior and identify significant deviations as potential intrusions, making them more suitable for dynamic and heterogeneous environments such as IoT networks [33].

The development of IDS for IoT environments presents additional challenges associated with the computational constraints of devices, including limitations in memory, processing power, and energy consumption. Furthermore, real-time applications require low latency and rapid response capabilities to prevent the large-scale propagation of attacks. Consequently, lightweight and scalable solutions have been extensively investigated in the literature, particularly those supported by Machine Learning techniques and Edge Computing paradigms [28, 55].

2.2 Machine Learning Applied to IDS in IoT

Machine Learning (ML) techniques applied to Intrusion Detection Systems (IDS) in IoT environments can generally be categorized into supervised learning, unsupervised learning, and Deep Learning-based approaches. Each category offers distinct advantages depending on data availability, computational resources, and the characteristics of the target application.

Machine Learning (ML) has become one of the most widely adopted approaches for developing intelligent Intrusion Detection Systems (IDS) in IoT environments due to its ability to automatically identify complex attack patterns from network traffic data. Unlike traditional signature-based IDS, which rely on predefined attack signatures and require frequent manual updates, ML-based IDS can generalize from historical observations and detect previously unseen attacks by learning statistical relationships among network features. This capability is particularly important in IoT ecosystems, where the diversity of devices, communication protocols, and attack vectors makes maintaining signature databases increasingly challenging. Recent surveys indicate that ML-based IDS have consistently achieved higher detection rates and lower false alarm rates than conventional approaches, particularly when trained using representative and well-balanced datasets such as ToN-IoT, CICIDS2017, and NSL-KDD. Consequently, ML has become the predominant paradigm adopted in contemporary IDS research for IoT security, serving as the foundation for more advanced approaches, including Deep Learning and Federated Learning [3, 25, 55].

In supervised methods, models are trained using previously labeled data, learning patterns associated with legitimate and malicious traffic. Algorithms such as Decision Trees and Random Forest stand out for their high classification performance, interpretability, and relatively low computational cost, characteristics that are particularly important for applications deployed on edge devices and resource-constrained environments [6, 28].

Among supervised learning algorithms, ensemble methods have received considerable attention due to their robustness, scalability, and high predictive performance in cybersecurity applications. Random Forest is one of the most frequently adopted classifiers for IoT intrusion detection because it combines multiple decision trees using bootstrap aggregation (bagging), thereby reducing overfitting while improving classification accuracy and model generalization. In contrast, Logistic Regression remains an important baseline algorithm owing to its low computational complexity, ease of implementation, and high interpretability, making it particularly suitable for resource-constrained IoT devices. More recently, Multilayer Perceptron (MLP) neural networks have demonstrated promising performance by effectively learning nonlinear relationships within network traffic data. However, selecting an appropriate classifier requires balancing detection accuracy, computational overhead, memory consumption, and inference latency, especially for real-time intrusion detection deployed in Edge Computing environments. Consequently, no single learning algorithm can be considered universally optimal, and model selection should be guided by the specific characteristics of the target IoT application and dataset [6, 16, 28, 33].

On the other hand, unsupervised methods, such as K-means and DBSCAN, do not rely on labeled data during training. These approaches aim to identify natural groupings within the data or detect instances considered anomalous with respect to the prevailing network behavior. In IoT scenarios, such methods are especially relevant due to the difficulty of obtaining large volumes of labeled data and the continuous evolution of attack

patterns [25, 68].

In addition to traditional ML approaches, Deep Learning (DL) techniques have also been explored for IoT-based IDS. Recurrent neural networks, autoencoders, and hybrid architectures have demonstrated high performance in detecting complex attacks and malicious traffic. Recent studies have combined deep learning with technologies such as blockchain and Federated Learning to enhance security while preserving the privacy of distributed data [7, 16, 65]. However, these approaches often require greater computational resources, which may limit their deployment on resource-constrained edge devices.

Despite the remarkable advances achieved by centralized Machine Learning and Deep Learning models in IoT intrusion detection, several challenges remain unresolved. IoT environments are inherently distributed, consisting of heterogeneous devices that continuously generate sensitive data under strict computational and communication constraints. Collecting all data in a centralized server may introduce privacy concerns, increase communication overhead, and limit scalability. Consequently, recent research has progressively shifted toward privacy-preserving and distributed learning paradigms, particularly Federated Learning, which enables collaborative model training without requiring raw data sharing among participating devices. Although Federated Learning is beyond the scope of the present study, the centralized evaluation conducted in this work establishes a reliable performance baseline that will support future investigations on distributed intrusion detection frameworks for IoT environments [16, 26, 37, 42].

2.3 Federated Learning Applied to IDS in IoT

Federated Learning (FL) has emerged as a promising approach for distributed training of Machine Learning models without requiring data centralization. In this paradigm, local devices perform training using their own data and share only the updated model parameters with a central server, reducing risks associated with privacy breaches and the exposure of sensitive information [37].

In IoT environments, FL offers important advantages due to the distributed nature of networks and the growing concern regarding data privacy and security. In addition to reducing the transmission of sensitive information to centralized servers, Federated Learning enables collaborative training among heterogeneous and geographically distributed devices [26, 32].

Several recent studies have investigated the application of FL to IDS for IoT environments. Bhavsar et al. proposed FL-IDS, a Federated Learning-based intrusion detection system for Transportation IoT environments, demonstrating improvements in both privacy preservation and distributed performance [16]. Other studies have explored hybrid models combining deep neural networks and FL to enhance attack detection capabilities in decentralized environments [59, 67].

Despite recent advances, significant challenges remain regarding data heterogeneity across clients, communication overhead, device synchronization, and computational constraints in edge environments. Consequently, current research efforts focus on developing lighter, more efficient, and more robust models to support the practical deployment of FL in real-world IoT scenarios [4, 48].

2.4 Datasets for IDS in IoT

The evaluation of Machine Learning-based IDS relies directly on the availability of representative datasets. Among the most widely used datasets in the literature are NSL-KDD, UNSW-NB15, CICIDS2017, and ToN-IoT [40, 55].

NSL-KDD is an evolution of the traditional KDD Cup 1999 dataset and remains widely used due to its reduced redundancy and improved balance between normal and malicious classes. Although it does not fully represent contemporary traffic in IoT environments, the dataset continues to be relevant for the initial evaluation of intrusion detection algorithms [55].

UNSW-NB15 and CICIDS2017, in turn, incorporate more modern attack scenarios and traffic characteristics that are closer to those observed in contemporary real-world networks. The ToN-IoT dataset stands out specifically for encompassing IoT and Industrial IoT environments, including sensor data, telemetry information, and various types of distributed attacks, making it an important benchmark in recent research on IDS and Federated Learning [22, 40].

The use of multiple datasets enables the evaluation not only of the predictive performance of models but also of their robustness and generalization capability across heterogeneous scenarios [28, 55].

2.5 Synthesis of Related Work and Research Gap

Recent studies on intrusion detection in IoT environments have demonstrated significant advances in the use of Machine Learning, Deep Learning, and Federated Learning for the identification of cyberattacks. Supervised models frequently achieve high Accuracy in scenarios with labeled data, while unsupervised and deep learning-based approaches have been employed

for anomaly detection and the identification of previously unknown threats [25, 28, 33].

The reviewed literature demonstrates that Machine Learning has become the predominant approach for intrusion detection in IoT environments, consistently outperforming traditional signature-based detection methods in terms of adaptability and detection accuracy. Most recent studies employ supervised learning algorithms, particularly Random Forest, Support Vector Machines, Gradient Boosting, and Deep Neural Networks, achieving high classification performance across publicly available datasets. Furthermore, recent investigations have increasingly explored Federated Learning as a privacy-preserving alternative to centralized training, enabling collaborative model development without exposing sensitive network traffic data. These advances highlight the growing maturity of ML-based IDS while simultaneously revealing new research challenges associated with scalability, data heterogeneity, privacy preservation, and deployment in distributed IoT environments [3, 16, 28, 42, 55].

Despite the significant progress achieved by recent studies, several research gaps remain open. Most existing works evaluate intrusion detection models using a single IoT dataset or focus on a limited set of attack scenarios, making it difficult to assess the robustness and generalization capability of the proposed approaches across heterogeneous IoT devices. In addition, many Federated Learning-based solutions employ computationally intensive Deep Learning architectures, which may be unsuitable for deployment on resource-constrained edge devices. Another limitation is that comparative analyses involving multiple IoT device categories under a unified experimental methodology remain relatively scarce. These observations indicate the need for systematic baseline studies that evaluate conventional Machine Learning algorithms across diverse IoT scenarios before investigating the additional benefits introduced by Federated Learning. Establishing such baselines provides a reliable reference for future comparisons involving distributed learning architectures and contributes to a better understanding of the trade-offs between predictive performance, computational efficiency, scalability, and privacy preservation in IoT intrusion detection systems [16, 22, 28, 42, 55].

Unlike many previous studies that primarily emphasize maximizing predictive performance through increasingly complex learning architectures, this work focuses on providing a systematic experimental evaluation of conventional Machine Learning algorithms across multiple IoT device categories using a consistent experimental protocol. By comparing Logistic Regression, Random Forest, and Multilayer Perceptron models under identical preprocessing procedures and evaluation metrics, this study establishes a reliable baseline for future investigations involving Federated Learning-based intrusion detection systems. Such an experimental foundation facilitates a more objective assessment of the benefits and limitations introduced by distributed learning approaches while supporting the development of scalable, privacy-preserving, and computationally efficient IDS solutions for heterogeneous IoT environments.

In this context, the present work investigates the application of Machine Learning techniques to IDS for IoT environments while simultaneously considering predictive performance, computational cost, and deployment feasibility in edge environments. In addition, the study takes into account recent advances in the literature on Federated Learning and the challenges associated with distributed security in IoT ecosystems, contributing to the discussion of lighter, more scalable solutions suitable for resource-constrained devices. Although the present study initially adopts centralized Machine Learning approaches, the future incorporation of Federated Learning-based strategies represents a promising direction for enhancing privacy, scalability, and suitability for distributed IoT environments.

3 Methodology

This work investigates the application of Machine Learning techniques to Intrusion Detection Systems (IDS) for IoT environments, focusing on predictive performance through experimental evaluation. Furthermore, the study establishes a preliminary centralized baseline intended to support future implementations of Federated Learning (FL) for distributed IDS applications in IoT networks.

The methodology was organized into sequential stages involving dataset selection, data preprocessing, model training, and experimental evaluation, establishing a reproducible baseline for future investigations involving Federated Learning and Edge Computing environments.

3.1 Proposed Architecture

The architecture considered in this work is based on a distributed IoT environment composed of edge devices responsible for network traffic collection and analysis. Initially, the models are trained and evaluated in a centralized manner, establishing an experimental baseline for performance comparison.

Subsequently, a Federated Learning-based architecture is proposed, in which multiple devices perform local training using their own data and share only the updated model parameters with a central server responsible for global aggregation. This approach reduces the need for direct data sharing, contributing to privacy preservation and reduced network traffic, as discussed in recent studies from the literature [26, 32, 37].

The proposed architecture follows the client-server paradigm commonly adopted in recent federated approaches for intrusion detection in IoT environments [4, 16].

The selected subsets were intentionally chosen because they represent distinct IoT application domains and different categories of connected devices, including industrial communication, environmental monitoring, smart home automation, and location-based services. This diversity allows the proposed models to be evaluated under heterogeneous traffic patterns and attack behaviors, providing a more comprehensive assessment of their robustness and generalization capability before future Federated Learning experiments.

3.2 Datasets Used

For the experimental evaluation, the ToN-IoT (Telemetry of Things and Industrial Internet of Things) dataset was employed, as it has been widely used in recent research on intrusion detection in IoT and IIoT environments. The dataset includes data collected from real IoT devices, sensors, industrial systems, and multiple categories of cyberattacks, enabling the evaluation of model behavior across heterogeneous scenarios.

In this work, specific subsets of the ToN-IoT dataset were utilized, including the Weather, Modbus, Garage Door, and GPS Tracker devices. Each subset presents distinct traffic and telemetry characteristics, allowing the analysis of detection capabilities under different application contexts.

The Weather subset contains information related to temperature, atmospheric pressure, and humidity. The Modbus subset comprises records associated with the Modbus industrial protocol, which is widely used in industrial automation systems. The Garage Door and GPS Tracker subsets represent typical IoT devices found in residential and tracking environments, respectively.

The use of multiple devices enables the assessment of model robustness in the presence of the heterogeneity that characterizes modern IoT environments and establishes an experimental baseline for future evaluations involving Federated Learning-based architectures.

Table 1: Characteristics of the ToN-IoT Subsets Used

Subset	**Inst.**	**Attributes**	**Class**
Modbus	31,106	FC1, FC2, FC3, FC4	N/A
Weather	39,260	Temperature, Pressure, Humidity	N/A
Garage Door	39,587	Door State, Smartphone Signal	N/A
GPS Tracker	38,960	Latitude, Longitude	N/A

Table 2: Class Distribution Across the Evaluated Subsets

Subset	Normal	Attack
Modbus	15.000	16.106
Weather	15.000	24.260
Garage Door	15.000	24.587
GPS Tracker	15.000	23.960

3.3 Data Preprocessing

Initially, the selected subsets of the ToN-IoT dataset were loaded. Attributes related to date and time were removed from the experiments because they do not represent characteristics directly associated with attack behavior.

To ensure the reproducibility of the experiments, all train-test splits were performed using a fixed random seed (`random_state = 42`). In addition, machine learning models with stochastic components, such as Random Forest and Multilayer Perceptron (MLP), were configured with the same random seed whenever applicable.

For the classification experiments, a binary classification approach was adopted, using the *label* variable as the target attribute, where the value 0 represents normal traffic and the value 1 represents malicious traffic.

The data were divided into training and testing sets using an 80%/20% split, with class stratification applied to preserve the original class distribution.

For models requiring feature normalization, the StandardScaler technique was employed to standardize the data with zero mean and unit variance. This procedure was primarily applied to Logistic Regression and Artificial Neural Network-based models.

3.4 Machine Learning Models

Three supervised models widely used in classification tasks were evaluated: Logistic Regression, Random Forest, and Multilayer Perceptron (MLP).

Logistic Regression was employed as a baseline classifier due to its computational efficiency, high interpretability, and widespread use in binary classification problems. The algorithm estimates the probability

that an instance belongs to a particular class by applying a logistic (sigmoid) function to a linear combination of the input features. Its low computational complexity makes it particularly suitable for real-time intrusion detection in resource-constrained IoT environments. Although its linear decision boundary may limit performance when modeling highly complex attack patterns, Logistic Regression provides a reliable reference for comparing more sophisticated Machine Learning models under identical experimental conditions [28, 33].

Random Forest was selected because of its robustness and ability to model complex nonlinear relationships commonly found in IoT network traffic. As an ensemble learning algorithm, it constructs multiple decision trees using bootstrap sampling and random feature selection, combining their predictions through majority voting to improve classification accuracy and generalization. This strategy reduces overfitting while maintaining strong predictive performance across heterogeneous datasets. In IoT intrusion detection, Random Forest has consistently achieved high accuracy, robustness against noisy data, and efficient training, making it one of the most widely adopted classifiers in recent IDS research. These characteristics justify its selection as one of the primary models evaluated in this study [3, 16, 22, 28].

The Multilayer Perceptron (MLP) was included in this study because of its capability to model complex nonlinear relationships that frequently characterize network traffic generated by IoT devices. As a feedforward artificial neural network composed of interconnected neurons organized into input, hidden, and output layers, the MLP learns decision boundaries through the backpropagation algorithm, iteratively adjusting connection weights to minimize the classification error. Compared with linear models, MLPs generally provide greater flexibility for detecting sophisticated attack patterns; however, they also require higher computational resources, careful hyperparameter tuning, and longer training times. Despite these limitations, MLPs have become one of the most widely adopted Deep Learning models for intrusion detection and provide an important benchmark for evaluating the trade-off between predictive performance and computational efficiency in IoT security applications [3, 16, 28].

All models were implemented using the Scikit-Learn library and evaluated under the same experimental conditions. Unless otherwise specified, the default hyperparameters provided by the Scikit-Learn library were adopted to establish a standardized experimental baseline, allowing a fair comparison among the evaluated algorithms while avoiding the influence of extensive hyperparameter tuning on the performance analysis.

Logistic Regression was configured using the *lbfgs* solver. Random Forest was configured with 100 decision trees. The MLP model was trained using a single hidden layer with 100 neurons and a maximum limit of 300 training epochs.

Table 3: Configuration of the Evaluated Models

Model	Configuration
Logistic Regression	solver = lbfgs
Random Forest	n_estimators = 100
MLP	hidden_layer_sizes = (100), max_iter = 300

3.5 Federated Learning

Although the primary focus of this stage of the study is the centralized evaluation of Machine Learning models, the experiments were designed to serve as a baseline for future implementations based on Federated Learning.

The proposed approach consists of distributing subsets of the ToN-IoT dataset among different simulated clients, representing distinct IoT devices. Each client performs local training using its own data and shares only the updated model parameters with a central server responsible for global aggregation.

For aggregating the local models, the Federated Averaging (FedAvg) strategy will be adopted, as it is one of the most widely used approaches in Federated Learning systems due to its simplicity and efficiency [37].

This approach reduces the need for direct data sharing, thereby contributing to privacy preservation and reducing communication overhead among participating devices [26, 32].

Therefore, the results presented in this work represent an essential initial step toward future evaluations involving Federated Learning applied to intrusion detection in distributed IoT environments [16].

3.6 Experimental Environment

The experiments were developed using the Python programming language and executed in a Jupyter Notebook environment.

The Pandas library was employed for data manipulation, NumPy for numerical operations, and Scikit-Learn for the implementation of Machine Learning algorithms and model evaluation.

The experiments were conducted in a conventional computing environment in order to validate the feasibility of the proposed methodology before implementing distributed scenarios based on Federated Learning.

4 Results

The experiments were conducted using four subsets of the ToN-IoT dataset: Modbus, Weather, Garage Door, and GPS Tracker. Three supervised Machine Learning algorithms were evaluated: Logistic Regression, Random Forest, and Multilayer Perceptron (MLP).

The models were trained and evaluated on binary classification tasks, considering normal traffic and malicious traffic. Performance was analyzed using the metrics Accuracy, Precision, Recall, and F1-Score. Table 4 summarizes the Accuracy results obtained by the evaluated algorithms across the different subsets of the ToN-IoT dataset.

Table 4: Model Accuracy Across the ToN-IoT Subsets

Subset	LR	MLP	RF
Modbus	51.41%	57.65%	98.46%
Weather	60.93%	80.41%	98.47%
Garage Door	100.00%	100.00%	100.00%
GPS Tracker	100.00%	100.00%	100.00%

LR: Logistic Regression; RF: Random Forest.

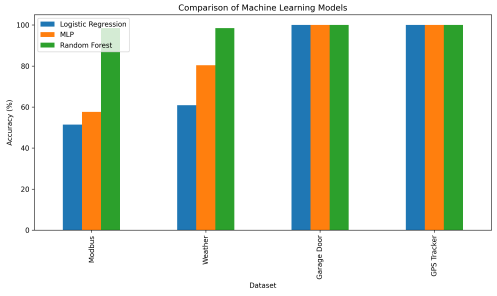


Figure 1: Comparison of the Accuracy of the Evaluated Models Across the ToN-IoT Subsets.

Table 5: Random Forest Performance Across ToN-IoT Subsets

Subset	Acc.	Prec.	Rec.	F1
Modbus	98.46%	0.99	0.98	0.98
Weather	98.47%	0.99	0.99	0.99
Garage Door	100.00%	1.00	1.00	1.00
GPS Tracker	100.00%	1.00	1.00	1.00

Random Forest consistently achieved the highest performance across all evaluated ToN-IoT subsets, obtaining accuracy values above 98% for the Modbus and Weather datasets and perfect classification performance for the Garage Door and GPS Tracker subsets. This superior performance can be attributed to the algorithm's ensemble learning strategy, which effectively captures complex and nonlinear relationships present in heterogeneous IoT network traffic. Similar findings have been reported in previous studies, where Random Forest demonstrated high robustness and predictive performance for intrusion detection in IoT environments [22, 28].

Logistic Regression exhibited lower performance on the Modbus and Weather datasets, suggesting limitations in modeling the more complex patterns present in these devices. For example, in the Modbus subset, the model achieved an Accuracy of only 51.41%, whereas Random Forest reached 98.46%.

The MLP model achieved intermediate results. Although it outperformed Logistic Regression on the Weather subset, reaching an Accuracy of 80.41%, its performance remained below that achieved by Random Forest.

These results demonstrate that different IoT devices present distinct levels of complexity for intrusion detection, directly influencing the performance of the evaluated algorithms.

5 Discussion

The results obtained reveal significant differences among the evaluated ToN-IoT subsets.

While the Modbus and Weather devices presented more challenging classification scenarios, the Garage Door and GPS Tracker subsets exhibited a high degree of class separability, enabling all evaluated models to achieve 100% Accuracy. Exploratory data analysis indicated that the attributes of these devices display markedly distinct patterns between normal and malicious traffic, facilitating correct class identification by the evaluated algorithms.

For the Modbus subset, Random Forest substantially outperformed the other algorithms, achieving an Accuracy of 98.46%. This result suggests that the attack patterns associated with the Modbus protocol exhibit nonlinear characteristics that are more effectively captured by decision tree-based models.

The Weather subset exhibited intermediate behavior. Although Logistic Regression achieved an Accuracy of only 60.93%, the MLP model reached 80.41%, indicating that techniques capable of modeling nonlinear relationships are better suited to capturing the patterns present in environmental sensor data.

For the Garage Door and GPS Tracker subsets, all algorithms achieved perfect performance. Exploratory analysis revealed a high degree of separability between the normal and attack classes, substantially reducing the complexity of the classification task. No evidence of data leakage was identified during data preprocessing

or model evaluation, indicating that the perfect classification results are consistent with the strong class separability observed in these subsets.

Overall, the experiments demonstrate that the selection of a Machine Learning model should take into account the specific characteristics of the monitored device and the dataset being analyzed. Among the evaluated algorithms, Random Forest exhibited the most consistent behavior, making it a strong candidate for future implementations in Federated Learning environments.

The experiments also highlight the importance of evaluating multiple devices and scenarios before deploying distributed architectures based on Federated Learning. Consequently, the results obtained in this stage provide an experimental baseline for future comparative studies.

6 Threats to Validity

The primary threats to the validity of this study are related to the use of only four subsets of the ToN-IoT dataset (Weather, Modbus, Garage Door, and GPS Tracker), the evaluation of a limited number of supervised algorithms, and the absence of experiments in a federated environment at this stage of the research.

Although the selected subsets represent different IoT devices and enable the evaluation of heterogeneous scenarios, other devices available within the ToN-IoT dataset or in alternative datasets may exhibit different characteristics, potentially affecting model performance.

Furthermore, the experiments were conducted in a centralized environment and therefore do not account for specific aspects of Federated Learning architectures, such as client heterogeneity, communication overhead, device synchronization, and the impact of distributed model aggregation.

Consequently, future studies involving a broader range of IoT devices, additional datasets, and Federated Learning-based implementations will be necessary to enhance the generalizability of the results obtained.

Another threat to validity is related to the class imbalance observed in some subsets of the ToN-IoT dataset, which may influence classifier performance and favor aggregate metrics such as Accuracy.

In addition, the experiments employed only a single stratified train-test split, and therefore the reported results should be interpreted as an initial experimental baseline. Techniques such as stratified cross-validation may be adopted in future studies to reduce potential variations resulting from data sampling and to further strengthen the robustness of the evaluation.

7 Conclusion

This work investigated the application of Machine Learning techniques for intrusion detection in IoT environments using subsets of the ToN-IoT dataset. Logistic Regression, Random Forest, and Multilayer Perceptron (MLP) models were evaluated in binary classification tasks involving normal and malicious traffic.

The experimental results revealed significant differences among the evaluated devices. While the Garage Door and GPS Tracker subsets exhibited high class separability, allowing all models to achieve 100% Accuracy, the Modbus and Weather subsets presented more challenging scenarios. In these cases, Random Forest achieved superior performance, reaching approximately 98% Accuracy and outperforming the other evaluated algorithms.

The obtained results established a reproducible initial experimental baseline for future evaluations involving Federated Learning-based architectures. Furthermore, the findings demonstrated that different IoT devices may present distinct levels of complexity for intrusion detection, reinforcing the importance of selecting appropriate algorithms according to the characteristics of the monitored environment. This baseline provides a consistent reference for future comparisons between centralized and federated intrusion detection approaches.

As future work, a federated architecture based on the Federated Averaging (FedAvg) algorithm will be implemented, distributing the training process across multiple simulated IoT devices. This will enable the evaluation of the impact of distributed training on intrusion detection performance and facilitate comparisons between centralized and federated models in Edge Computing environments.

Artifact Availability

The source code, experimental notebook, scripts, results, and supplementary materials required to reproduce the experiments presented in this study are publicly available at:

Project Repository

References

[1] Adasme, P., Viveros, A., Ayub, M. S., Soto, I., Firoozabadi, A. D., and Rodríguez, D. Z. A multiple linear regression approach to optimize the worst user capacity and power allocation in a wireless network. In *2023 South American Conference On Visible Light Communications (SACVLC)*, pages 6–11. IEEE, 2023.

[2] Adasme, P., Viveros, A., Soto, I., Firoozabadi, A. D., and Rodríguez, D. Z. Exploring worst arc flow minimization: A comparative study of a provided wireless network and its derivation via spanning tree topology. In *International Conference on Mobile Web and Intelligent Information Systems*, pages 55–66. Springer, 2024.

[3] Alfahaid, A., Alalwany, E., Almars, A. M., Alharbi, F., Atlam, E., and Mahgoub, I. Machine learning-based security solutions for iot networks: A comprehensive survey. *Sensors*, 25(11), 2025.

[4] Alghamdi, A. et al. An optimal federated learning-based intrusion detection for iot environment. *Scientific Reports*, 15, 2025.

[5] Alkali, Y., Routray, I., and Whig, P. Study of various methods for reliable, efficient and secured iot using artificial intelligence. In *Proceedings of the International Conference on Innovative Computing & Communication (ICICC)*, 2022.

[6] Alomiri, A., Mishra, S., and AlShehri, M. Machine learning-based security mechanism to detect and prevent cyber-attack in iot networks. *International Journal of Computing and Digital Systems*, 16(1):645–659, 2024.

[7] Alsharif, N. A., Mishra, S., and Alshehri, M. Ids in iot using machine learning and blockchain. *Engineering, Technology & Applied Science Research*, 13(4):11197–11203, 2023.

[8] Alyami, H. et al. Deep learning and federated learning for iot security: A survey. *Electronics*, 12(9):2103, 2023.

[9] Alzhrani, R. and Alliheedi, M. Enhancing iot security in 5g networks: Mitigating ddos attacks with deep learning. *Journal of Information Security and Cybercrimes Research*, 7(2):156–166, 2024.

[10] Awotunde, J. B., Sur, S. N., Imoize, A. L., Rodríguez, D. Z., and Akanji, B. An enhanced keylogger detection systems using recurrent neural networks enabled with feature selection model. In *International Conference on Communication, Devices and Networking*, pages 525–539. Springer, 2024.

[11] Ayub, M. S., Adasme, P., Melgarejo, D. C., Rosa, R. L., and Rodríguez, D. Z. Intelligent hello dissemination model for fanet routing protocols. *IEEE Access*, 10:46513–46525, 2022.

[12] Ayub, M. S., Adasme, P., Rodriguez, D. Z., Saadi, M., Shongwe, T., and Kanadilovna, A. Z. Expanding horizon: The role of reconfigurable intelligent surfaces in enabling massive connectivity. *2024 Horizons of Information Technology and Engineering (HITE)*, pages 1–6, 2024.

[13] Ayub, M. S., Adasme, P., Shongwe, T., Rodriguez, D. Z., Rosa, R. L., Iqbal, M., and Pan, J.-Y. Fusing reconfigurable intelligent surfaces with 6g non-terrestrial networks. In *2024 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pages 1–6. IEEE, 2024.

[14] Batista, A. P., Ayub, M. S., Adasme, P., Begazo, D. C., Shad, M. R., Saadi, M., Rosa, R. L., and Rodríguez, D. Z. A methodology for estimating radiofrequency signal attenuation from rainfall and atmospheric gases in 5g-and-beyond networks. *IET Networks*, 14(1):e70000, 2025.

[15] Bharati, S. and Podder, P. Machine and deep learning for iot security and privacy: applications, challenges, and future directions. *Security and communication networks*, 2022(1):8951961, 2022.

[16] Bhavsar, M. H., Bekele, Y. B., Roy, K., Kelly, J. C., and Limbrick, D. Fl-ids: Federated learning-based intrusion detection system using edge devices for transportation iot. *IEEe Access*, 12:52215–52226, 2024.

[17] Canadian Institute for Cybersecurity. Cicids2017 dataset, 2017. University of New Brunswick.

[18] Chaudhary, S., Wuttisittikulkij, L., Saadi, M., Sharma, A., Al Otaibi, S., Nebhen, J., Rodriguez, D. Z., Kumar, S., Sharma, V., Phanomchoeng, G., et al. Coherent detection-based photonic radar for autonomous vehicles under diverse weather conditions. *PLoS one*, 16(11):e0259438, 2021.

[19] Cordero, S., Adasme, P., Dehghan Firoozabadi, A., Rosa, R. L., and Rodríguez, D. Z. Mathematical models for coverage with star tree backbone topology for 5g millimeter waves networks. *Symmetry*, 17(1):141, 2025.

[20] Da Silva, S. E. I., Rodriguez, D. Z., Rosa, R. L., Adasme, P., and Saadi, M. Ai/ml-enhanced security monitoring for 5g-enabled big data sensor networks. In *2024 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pages 1–6. IEEE, 2024.

[21] de Sousa, A. L., OKey, O. D., Rosa, R. L., Saadi, M., and Rodriguez, D. Z. A novel resource allocation in software-defined networks for iot application. In *2023 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pages 1–5. IEEE, 2023.

[22] Gad, A. R., Haggag, M., Nashat, A. A., and Barakat, T. M. A distributed intrusion detection system using machine learning for iot based on ton-iot dataset. *International Journal of Advanced Computer Science and Applications*, 13(6), 2022.

[23] Gassais, R., Ezzati-Jivan, N., Fernandez, J. M., Aloise, D., and Dagenais, M. R. Multi-level host-based intrusion detection system for internet of things. *Journal of Cloud Computing*, 9(1):62, 2020.

[24] Gonçalves, J. G., Ayub, M. S., Zhumadillayeva, A., Dyussekeyev, K., Ayimbay, S., Saadi, M., Lopes Rosa, R., and Rodríguez, D. Z. Decentralized machine learning framework for the internet of things: Enhancing security, privacy, and efficiency in cloud-integrated environments. *Electronics*, 13(21):4185, 2024.

[25] Haji, S. H. and Ameen, S. Y. Attack and anomaly detection in iot networks using machine learning techniques: A review. *Asian journal of research in computer science*, 9(2):30–46, 2021.

[26] Kairouz, P., McMahan, H. B., Avent, B., et al. Advances and open problems in federated learning. *Foundations and Trends in Machine Learning*, 14(1–2):1–210, 2021.

[27] Karthikeyan, M., Manimegalai, D., and RajaGopal, K. Firefly algorithm based wsn-iot security enhancement with machine learning for intrusion detection. *Scientific Reports*, 14(1):231, 2024.

[28] Kaushik, S., Bhardwaj, A., Almogren, A., Bharany, S., Altameem, A., Rehman, A. U., Hussen, S., and Hamam, H. Robust machine learning based intrusion detection system using simple statistical techniques in feature selection. *Scientific Reports*, 15(1):3970, Feb 1 2025.

[29] Khan, A. et al. Fedmade: Robust federated learning for intrusion detection in iot networks using a dynamic aggregation method. *arXiv preprint arXiv:2408.07152*, 2024.

[30] Khraisat, A. et al. Intrusion detection in iot based on machine learning and deep learning algorithms. *Sensors*, 21(14):4751, 2021.

[31] Latif, N., Saadi, M., and Rodriguez, D. Z. Semantic segmentation: Techniques, challenges, and applications in intelligent transportation systems. *Optical and Wireless Communications*, pages 153–179.

[32] Li, T., Sahu, A. K., Talwalkar, A., and Smith, V. Federated learning: Challenges, methods, and future directions. *IEEE Signal Processing Magazine*, 37(3):50–60, 2020.

[33] Malathi, C. and Padmaja, I. N. Identification of cyber attacks using machine learning in smart iot networks. *Materials Today: Proceedings*, 80:2518–2523, 2023.

[34] Mathew, U. O., Rodriguez, D. Z., Rosa, R. L., Ayub, M. S., and Adasme, P. Advancing healthcare 5.0 through federated learning: Opportunity for security enforcement using blockchain. In *2024 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pages 1–6. IEEE, 2024.

[35] Matthew, U. O., Rosa, R. L., Kazaure, J. S., Adesina, O. J., Oluwatimilehin, O. A., Oforgu, C. M., Asuni, O., Okafor, N. U., and Rodriguez, D. Z. Software-defined networks in iot ecosystems for renewable energy resource management. pages 1–5, 2024.

[36] Matthew, U. O., Rosa, R. L., Saadi, M., and Rodríguez, D. Z. Interpretable ai framework for secure and reliable medical image analysis in iomt systems. *IEEE Journal of Biomedical and Health Informatics*, 2025.

[37] McMahan, B., Moore, E., Ramage, D., Hampson, S., and Aguera y Arcas, B. Communication-efficient learning of deep networks from decentralized data. *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, pages 1273–1282, 2017.

[38] Mendonca, R. V., Silva, J. C., Rosa, R. L., Saadi, M., Rodriguez, D. Z., and Farouk, A. A lightweight intelligent intrusion detection system for industrial internet of things using deep learning algorithms. *Expert Systems*, 39(5):e12917, 2022.

[39] Mishra, S., Albarakati, A., and Sharma, S. K. Cyber threat intelligence for iot using machine learning. *Processes*, 10(12):2673, 2022.

[40] Moustafa, N. et al. The ton_iot datasets: A new generation of datasets for iot intrusion detection systems. *arXiv preprint arXiv:2008.02846*, 2020.

[41] Moustafa, N. and Slay, J. Unsw-nb15 dataset, 2015.

[42] Nguyen, M. et al. Federated learning for intrusion detection in iot environments: A privacy-preserving strategy. *Discover Internet of Things*, 2025.

[43] Okey, D. O., Dadkhah, S., Molyneaux, H., Rodríguez, D. Z., and Kleinschmidt, J. H. ipaseciot: An intelligent pipeline for automatic and adaptive feature extraction for secure iot device identification and intrusion detection. *Internet of Things*, page 101802, 2025.

[44] Okey, O. D., Maidin, S. S., Adasme, P., Lopes Rosa, R., Saadi, M., Carrillo Melgarejo, D., and Zegarra Rodríguez, D. Boostedenml: Efficient technique for detecting cyberattacks in iot systems using boosted ensemble machine learning. *Sensors*, 22(19):7409, 2022.

[45] Okey, O. D., Melgarejo, D. C., Saadi, M., Rosa, R. L., Kleinschmidt, J. H., and Rodriguez, D. Z. Transfer learning approach to ids on cloud iot devices using optimized cnn. *IEEE Access*, 11:1023–1038, 2023.

[46] Okey, O. D., Rodríguez, D. Z., Guimarães, F. G., and Kleinschmidt, J. H. Cafiks: Communication-aware federated ids with knowledge sharing for secure iot connectivity. *IEEE Access*, 2025.

[47] Okey, O. D., Rodriguez, D. Z., and Kleinschmidt, J. H. Enhancing iot intrusion detection with federated learning-based cnn-gru and lstm-gru ensembles. In *2024 19th International Symposium on Wireless Communication Systems (ISWCS)*, pages 1–6. IEEE, 2024.

[48] Onsu, M. A., Kantarci, B., and Boukerche, A. How to cope with malicious federated learning clients: an unsupervised learning-based approach. *Computer Networks*, 234:109938, 2023.

[49] Oriakhi, V. N., Nwaiku, M., Odubola, O. A., Muojekwu, E. E., Matthew, U. O., Rosa, R. L., and Rodriguez, D. Z. Clinical automation in the age of robotics: Hospital disinfection using 5g iot biomedical robots. In *Smart Technologies for Sustainable Development Goals*, pages 337–362. CRC Press, 2025.

[50] OYEDEMI, O., Rodriguez, D. Z., Rosa, R. L., and Ugochukwu, O. M. Containerization approach for secure internet of medical things (iomt) communication protocols. *INFOCOMP Journal of Computer Science*, 23(2), 2024.

[51] Oyedemi, O. A., Rosa, R. L., Matthew, U. O., Ogundele, L. A., Ogunwale, Y. E., and Rodríguez, D. Z. Privacy-preserving federated data governance framework for secure parameter exchange in distance education. In *2025 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pages 1–6. IEEE, 2025.

[52] Oyekunle, D., Ugochukwu, O. M., Rosa, R. L., Rodriguez, D. Z., and Fatai, L. O. Novel approaches in clinical simulation: Immersive educational technology to enhance nursing education. *INFOCOMP Journal of Computer Science*, 23(1), 2024.

[53] Paiva, H. W. A., Golçalves, J. G., Rodrígues, D. Z., and Rosa, R. L. A comprehensive analysis of virtual reality applications in healthcare. *INFOCOMP Journal of Computer Science*, 23(1), 2024.

[54] Rafael Câmara Araújo, A., Lopes Rosa, R., Zegarra Rodríguez, D., Sarah Maidin, S., Bamidele Awotunde, J., and Saadi, M. Lightbioptimum: An intrusion detection system based on bio-inspired algorithm for vanet. *Transactions on Emerging Telecommunications Technologies*, 36(10):e70254, 2025.

[55] Rahman, M. M., Shakil, S. A., and Mustakim, M. R. A survey on intrusion detection system in iot networks. *Cyber Security and Applications*, 3:100082, 2025.

[56] Ribeiro, D. A., Melgarejo, D. C., Saadi, M., Rosa, R. L., and Rodríguez, D. Z. A novel deep deterministic policy gradient model applied to intelligent transportation system security problems in 5g and 6g network scenarios. *Physical Communication*, 56:101938, 2023.

[57] S., B. and Nagapadma, R. RT-IoT2022 . UCI Machine Learning Repository, 2023. DOI: https://doi.org/10.24432/C5P338.

[58] Sanju, P. Enhancing intrusion detection in iot systems: A hybrid metaheuristics-deep learning approach with ensemble of recurrent neural networks. *Journal of Engineering Research*, 11(4):356–361, 2023.

[59] Sharma, P. et al. Edge-flguard: A federated learning framework for real-time anomaly detection in 5g-enabled iot ecosystems. *Applied Sciences*, 15(12):6452, 2025.

[60] Tavallaee, M. et al. Nsl-kdd dataset, 2009.

[61] Teodoro, A. A., Gomes, O. S., Saadi, M., Silva, B. A., Rosa, R. L., and Rodríguez, D. Z. An fpga-based performance evaluation of artificial neural network architecture algorithm for iot. *Wireless Personal Communications*, 127(2):1085–1116, 2022.

[62] Tien, C.-W., Huang, T.-Y., Chen, P.-C., and Wang, J.-H. Using autoencoders for anomaly detection and transfer learning in iot. *Computers*, 10(7):88, 2021.

[63] Torres, A., Rosa, R. L., Rodríguez, D. Z., and Saadi, M. Advancing neural speech codecs: Integrating psychoacoustic models for enhanced speech quality. In *2024 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pages 1–6. IEEE, 2024.

[64] Ugochukwu, O. M., Rosa, R. L., Adenike, O. O., and Rodriguez, D. Z. Advancing cybersecurity use of sensitive data in electronic healthcare system: A review of privacy and regulations. *INFOCOMP Journal of Computer Science*, 23(2), 2024.

[65] Vargas, H., Lozano-Garzon, C., Montoya, G. A., and Donoso, Y. Detection of security attacks in industrial iot networks: A blockchain and machine learning approach. *Electronics*, 10(21):2662, 2021.

[66] Zegarra Rodriguez, D., Daniel Okey, O., Maidin, S. S., Umoren Udo, E., and Kleinschmidt, J. H. Attentive transformer deep learning algorithm for intrusion detection on iot systems using automatic xplainable feature selection. *Plos one*, 18(10):e0286652, 2023.

[67] Zhang, W. et al. Fedmse: Semi-supervised federated learning approach for iot network intrusion detection. *arXiv preprint arXiv:2410.14121*, 2024.

[68] Zhang, Y. and Liu, Q. On iot intrusion detection based on data augmentation for enhancing learning on unbalanced samples. *Future Generation Computer Systems*, 133:213–227, 2022.