JCTA Journal of Computing Theories and Applications ISSN:3024-9104

Research Article

A Comparative Analysis of Supervised Machine Learning Algorithms for IoT Attack Detection and Classification

Jean Pierre Ntayagabiri [1,*], Youssef Bentaleb [2], Jeremie Ndikumagenge [3], and Hind El Makhtoum [4]

[1] Doctoral School of the University of Burundi, Center for Research in Infrastructure, Environment and Technology (CRIET), University of Burundi, Bujumbura, Burundi; e-mail : jpntayaga2@gmail.com
[2] Engineering Sciences Laboratory, ENSA Kenitra, Ibn Tofaïl University, Kenitra, Morocco; e-mail : ybentaleb@gmail.com
[3] Center for Research in Infrastructure, Environment and Technology (CRIET), University of Burundi, Bujumbura, Burundi; e-mail : jeremie.ndikumagenge@ub.edu.bi
[4] Engineering Sciences Laboratory, ENSA Kenitra, Ibn Tofaïl University, Kenitra, Morocco; e-mail : elmaktoum_hind@live.fr
* Corresponding Author : Jean Pierre Ntayagabiri

Abstract: The proliferation of Internet of Things (IoT) devices has introduced significant security challenges, necessitating robust attack detection mechanisms. This study presents a comprehensive comparative analysis of ten supervised learning algorithms for IoT attack detection and classification, addressing the critical challenge of balancing detection accuracy with practical deployment constraints. Using the CICIoT2023 dataset, encompassing data from 105 IoT devices and 33 attack types, we evaluate Naive Bayes, Artificial Neural Networks (ANN), Logistic Regression (LR), k-NN, XGBoost, Random Forest (RF), LightGBM, GRU, LSTM, and CNN algorithms based on some performance metrics. The comparative test results show superior performance to the traditional ensemble approach, with RF achieving 99.29% accuracy and leading precision (82.30%), followed closely by XGBoost with 99.26% accuracy and 79.60% precision. Deep learning approaches also demonstrate strong capabilities, with CNN achieving 98.33% accuracy and 71.18% precision, though these metrics indicate ongoing challenges with class imbalance. The analysis of confusion matrices reveals varying success across different attack types, with some algorithms showing perfect detection rates for certain attacks while struggling with others. The study highlights a crucial distinction in IoT security: while high precision remains important, the potentially catastrophic impact of missed attacks necessitates equal attention to recall metrics, as evidenced by the varying recall rates across algorithms (RF: 72.19%, XGBoost: 71.69%, CNN: 64.72%). These findings provide vital insights for developing balanced, context-aware intrusion detection systems for IoT environments, emphasizing the need to consider performance metrics and practical deployment constraints.

Keywords: Deep Learning; Internet of Things; Intrusion Detection; Machine Learning; Network Security; Supervised Learning.

Received: December, 13th 2024
Revised: February, 5th 2025
Accepted: February, 9th 2025
Published: February, 13th 2025

1. Introduction

The Internet of Things (IoT) has emerged as a cornerstone of global digital transformation, revolutionizing sectors including healthcare, industry, transportation, and smart cities. This technological paradigm enables critical processes such as remote medical monitoring, infrastructure management, and home automation through the interconnection of billions of devices. However, this massive interconnection also introduces significant cybersecurity vulnerabilities, making IoT infrastructures prime targets for attackers due to their inherent limitations: restricted resources, diverse protocols, and the absence of universal security standards [1], [2].

Previous research has explored various approaches to secure IoT environments[3]–[5]. While effective for predefined threats [6], traditional rule-based systems have proven insuffi-

cient for evolving and unknown attacks. Machine learning (ML) and deep learning (DL) approaches have gained prominence due to their ability to identify complex behavioral patterns from large datasets. Angelin et al.[6] demonstrated the effectiveness of Random Forests (RF) for IoT environments, while Mall et al. [7] highlighted the potential of Deep Neural Networks (DNNs) for real-time analysis. Ding et al.[8] and Halbouni et al. [9] proposed hybrid architectures combining Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks. Lightweight models have also been developed and evaluated for resource-constrained IoT devices[10]–[16] but often lack robustness for sophisticated attacks.

Each method presents distinct advantages and limitations. Rule-based systems offer interpretability but lack adaptability to new threats[17]. Deep learning approaches demonstrate superior detection capabilities but require significant computational resources [18]–[20]. Traditional ML algorithms provide a balance but may struggle with complex attack patterns [21]–[25]. Recent research by Kumar et al. [26] has explored unsupervised and semi-supervised techniques to address the impracticality of manual data labeling, introducing clustering algorithms and federated learning approaches.

The urgency of addressing these security challenges is underscored by high-profile incidents like the Mirai botnet attack in 2016, which disrupted large portions of the internet[27]–[32]. The proliferation of threats such as Distributed Denial of Service (DDoS) attacks, brute force attempts, spoofing, and malware targeting IoT devices can compromise sensitive data, cause service interruptions, or result in physical damage to critical infrastructures [33]–[37]. Current solutions often fail to balance detection accuracy with practical deployment constraints, particularly in resource-constrained environments.

To address these challenges, this study conducts a comprehensive comparative analysis of ten supervised learning algorithms for IoT attack detection and classification. The CICIoT2023 dataset [38], which includes data from 105 devices and 33 attack types, is utilized to evaluate and compare the performance of traditional ML and modern DL algorithms. This research makes several key contributions: (1) a systematic evaluation of algorithm performance across multiple metrics, including accuracy, precision, recall, and F1-score; (2) identification of optimal algorithms for specific deployment scenarios; (3) analysis of the impact of class imbalance on detection performance; and (4) practical recommendations for implementing intrusion detection systems in IoT environments.

The remainder of this article is structured as follows: Section 2 provides a detailed review of related work in IoT attack detection and classification. Section 3 outlines the research methodology and the CICIoT2023 dataset. Section 4 examines the performance comparison of supervised learning algorithms. Section 5 discusses the findings and their implications. Finally, Section 6 concludes with key contributions and future research directions.

2. Related Works

The field of cybersecurity for IoT systems has seen the emergence of numerous innovative methods aimed at improving attack detection and prevention. Meneghello et al. [1] discussed security threats in the IoT sector and proposed countermeasures such as encryption and intrusion detection systems (IDS). Additionally, Goel et al.[2] addressed IoT-specific vulnerabilities, while Koroniotis et al. [39] analyzed several machine-learning techniques using the UNSW-NB15 dataset to monitor malicious activities and trace botnets using unique identifiers. Similarly, Hodo et al. [40] explored using ANNs to detect DoS/DDoS attacks by distinguishing normal behaviors from attack patterns in a virtual environment. Ahmad et al. [4] investigated using RF and Extreme Learning Machines to enhance IDS accuracy.

Regarding feature optimization and false-positive reduction, Samriya et al. [41] proposed combining deep learning with nature-inspired algorithms such as min-max normalization and ant colony optimization to reduce data dimensionality. The work of Deshmukh et al. complemented this approach [42], and Javad et al. [43] integrated convolutional neural networks (CNNs) and autoencoders (AEs) to enhance IDS efficiency by reducing data features with autoencoders. In their publications, a number of authors have tested several machine learning algorithms on the UNSW NB15 and KDD99 datasets [44]–[50]. Furthermore, Pramilaranie et al.[51] proposed a cost-based random forest classifier (CRFC), which uses a cost matrix derived from feature importance to improve classification despite data imbalances.

Ge et al. [52] developed a framework to trace the origin of attacks, though their approach has not been tested for attack detection or false-positive evaluation. Additionally, Mahdavinejad et al. [53] surveyed machine learning algorithms to extract patterns from IoT data, highlighting challenges related to the scale and velocity of real-time data. Baich et al. [54] examined binary and multi-class classification for attacks, while Kumar et al. [55] proposed a fuzzy CNN-based IDS to improve communication security.

A similar approach is observed in the work of Sajid et al. [56], who discussed security issues in IoT cloud SCADA systems, emphasizing the importance of maintaining quality of service while ensuring security. In contrast, Samara et al. [57] studied intrusion detection techniques for IoT networks, highlighting the challenges connected devices pose.

Moreover, Xu et al. [58] utilized the recursive feature elimination (RFE) algorithm and the binary grey wolf heuristic optimizer (BGWO) to select the most relevant features, combining this approach with SMOTE to address data imbalances. Additionally, research by Yin et al. [59], which utilized RNNs to extract data representations for intrusion detection, demonstrated the effectiveness of recurrent neural networks for this task.

In botnet detection, Mbona et al. [60] demonstrated that machine learning techniques, combined with flow identifiers, were effective in identifying botnet intrusions. Their decision tree model achieved a false positive alert rate of 6.77%. Lastly, Beaver et al. [61] used machine learning methods to detect attacks in serial communications of remote endpoints, finding that nearest neighbors and RF performed best.

This study aims to deepen the understanding of the performance of supervised learning algorithms for attack classification in IoT systems. The focus is on the comparative analysis of different supervised learning algorithms, evaluating their ability to accurately classify various types of IoT attacks.

3. Research Method

3.1. Dataset Description and Collection

This research utilizes the CICIoT2023 dataset[38], a comprehensive collection of IoT network activity records designed explicitly for cybersecurity analysis. The dataset comprises 1,048,575 records across 47 columns, each representing distinct network flow characteristics essential for attack pattern detection and analysis.

The dataset encompasses several key categories of variables that provide comprehensive network traffic analysis capabilities. The temporal measurements include flow and session durations, inter-arrival time intervals, and header length measurements, offering detailed insights into the timing aspects of network communications. Network protocol indicators span across multiple layers, incorporating basic protocols such as TCP, UDP, ICMP, IPv, ARP, and DHCP, as well as application-level protocols including HTTP, HTTPS, DNS, Telnet, SMTP, SSH, and IRC. TCP flag measurements track connection states through fin, syn, rst, psh, ack, ece, and cwr flags. Statistical metrics provide deeper analytical capabilities through descriptive statistics such as total sums, minimums, maximums, averages, and standard deviations, complemented by advanced metrics, including magnitude, radius, covariance, variance, and weight calculations. The dataset also includes comprehensive transmission rate measurements across various network parameters.

3.2. Attack Distribution Analysis

The analysis of attack categories in the dataset reveals a complex and nuanced threat landscape, as illustrated in Figure 1. The distribution pattern indicates a clear hierarchy of threat prevalence, with a dominant attack category accounting for 15.38% of all recorded attacks. This is followed by a secondary significant threat category accounting for 11.56% of the total attacks. The intermediate threat landscape consists of several substantial attack categories, with representations of 9.66%, 8.81%, 8.74%, and 7.69%, respectively. These are complemented by less frequent but significant attack types, including 5.70% and 4.31% categories. The remainder of the attack landscape consists of several minor categories, each representing less than 3% of total attacks yet potentially indicating emerging or sophisticated threat vectors that warrant continued monitoring.

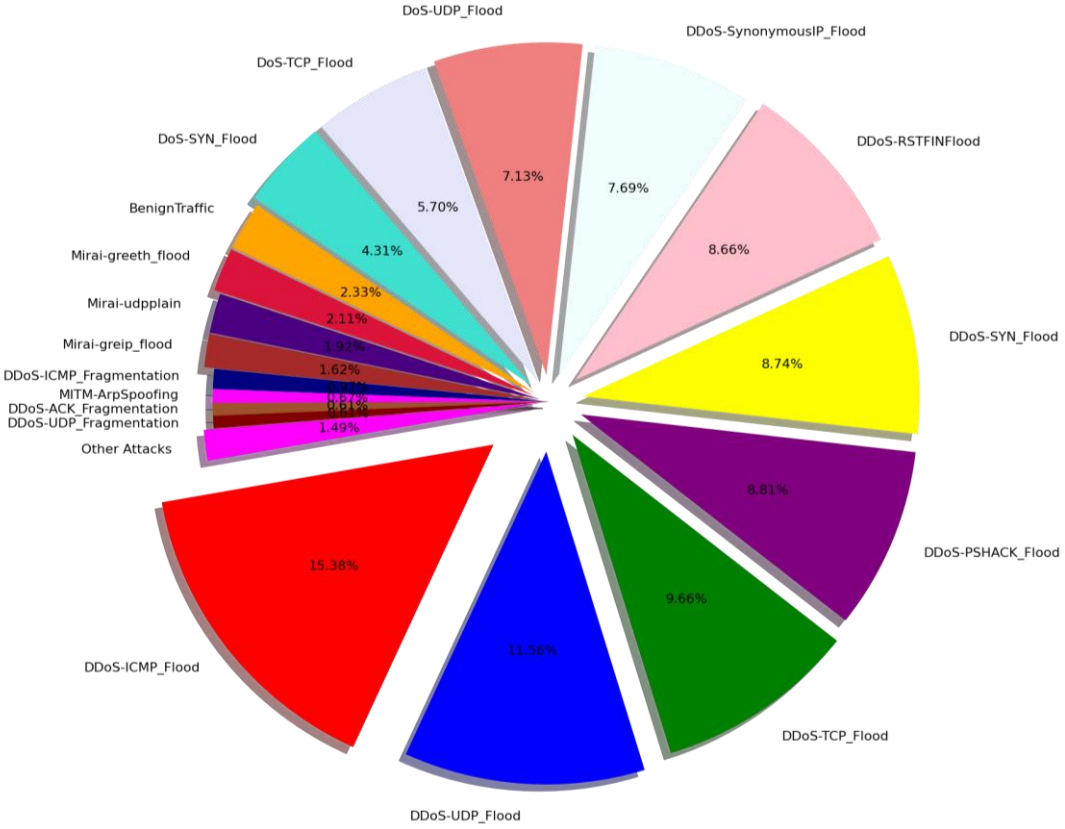

Figure 1. Distribution of different attack categories within a data set

3.3. Data Preprocessing Methodology

As illustrated in Figure 2, the data preprocessing process begins with acquiring a dataset from the IoT_Intrusion.csv file containing forty-seven features related to IoT network traffic. These features include flow metrics, protocol indicators, and traffic patterns. The initial data exploration and cleaning phase ensures data quality and identifies potential anomalies or missing values in the dataset.

Following data acquisition, we proceed with label encoding to transform categorical labels into numerical values, a necessary step for subsequent model training. Feature selection is then performed, focusing on several essential categories, including flow metrics such as duration and rate, protocol indicators like HTTP and HTTPS, flag counts, and various statistical measurements. Through feature importance analysis using ExtraTreesClassifier, the most relevant features are identified and retained to create a reduced feature set alongside the complete feature set[62].

The data is then strategically divided into training and testing sets, maintaining a 70% allocation for training and 30% for testing. A fixed random state is used to ensure result reproducibility. This division is performed before scaling to prevent data leakage between the sets. The final preprocessing phase involves a structured normalization process. First, StandardScaler is applied to the training data, centering it and scaling to unit variance—an essential step given the diversity of scales and units across features. The same scaling parameters derived from the training set are then applied to the test set to maintain consistency. This approach ensures that the test data remains unseen while preserving the statistical relationships within the dataset. This methodical preprocessing framework establishes a robust foundation for subsequent model training and evaluation, ensuring statistical validity and practical applicability for IoT intrusion detection.

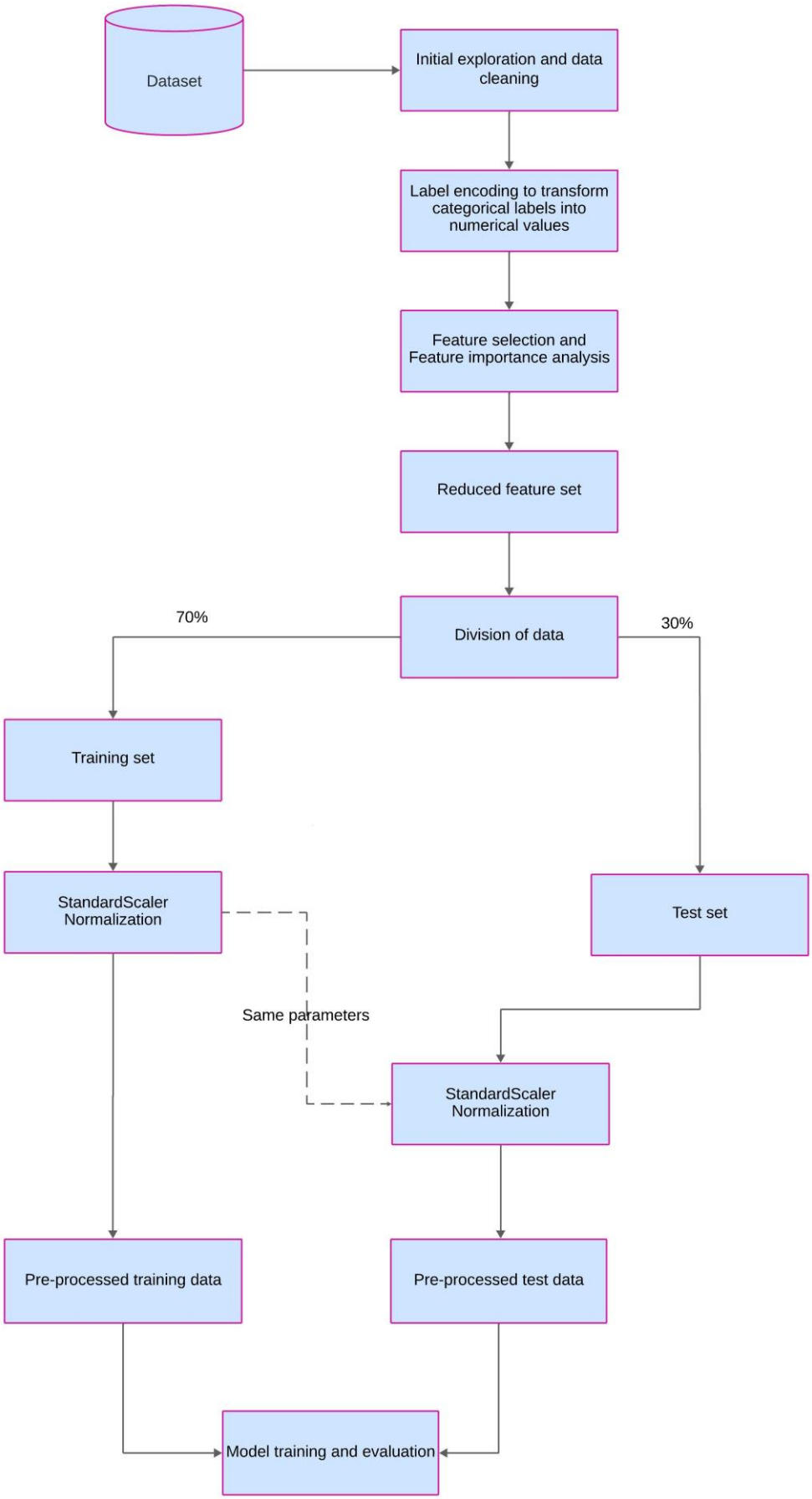

Figure 2. Data Preprocessing Methodology

3.4. Model Evaluation

3.4.1. Confusion Matrix

The confusion matrix is a key tool for evaluating classification models. It compares predictions to actual classes, showing true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN). This helps identify biases, especially in contexts like IoT attack detection, where errors can be critical.

3.4.2. Accuracy

Accuracy is the proportion of correct predictions over all samples, calculated using Equation (1).

$$accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

It is functional but misleading with imbalanced datasets, as it doesn't differentiate the performance of minority classes.

3.4.3. Precision

Precision calculates the model's ability to avoid false positives using Equation (2).

$$precission = \frac{TP}{TP + FP} \tag{2}$$

It is crucial when false alerts can lead to costs or disruptions. However, it doesn't account for false negatives, so it should be balanced with recall.

3.4.4. Recall

Recall measures the model's ability to detect all positive instances, calculated using Equation (3).

$$recall = \frac{TP}{TP + FN} \tag{3}$$

It is critical when false negatives are costly. However, high recall may lead to too many false alarms, requiring a balance with precision.

3.4.5. F1-score

The F1-score combines precision and recall into a single harmonic measure, calculated using Equation (4).

$$f1 = 2 \times \frac{precission \cdot recall}{precission + recall} \tag{4}$$

It is especially useful for imbalanced data, reflecting a good balance between attack detection and minimizing false alarms.

3.4.6. Receiver Operating Characteristic - Area Under Curve

The ROC curve evaluates the model's overall performance by plotting the true positive rate (TPR) against the false positive rate (FPR). The Area Under Curve (AUC) quantifies this performance, where 0.5 indicates random performance, and 1 indicates perfection. It is crucial for systems like IoT intrusion detection, allowing the comparison of models without setting a specific threshold.

4. Performance Evaluation of Different Supervised Learning Algorithms in Attack Detection and Classification

Detecting and classifying attacks are major challenges regarding network and IoT system security. These environments are exposed to various threats, ranging from Denial of Service (DoS) attacks to more complex intrusions such as malware-based attacks or ransomware. To meet these challenges, machine learning and deep learning algorithms have emerged as promising solutions, capable of analyzing massive volumes of data in real-time and detecting anomalous behavior with remarkable accuracy.

Evaluating the performance of these algorithms is a crucial step in designing and implementing an intrusion detection system (IDS). It enables us not only to compare the effective-

ness of different models but also to identify their strengths and weaknesses in specific contexts. For example, a model may excel in detecting rare attacks thanks to its high sensitivity but suffer from a high false positive rate, making it less practical to use in a real environment.

Metrics such as accuracy, recall, class-specific precision, and F1-score are often used to evaluate these models. These indicators help to understand how much a model can distinguish attacks from normal behavior while correctly minimizing misclassification. In addition, tools such as the confusion matrix and ROC-AUC curves offer an overview of model performance by considering the balance between different error categories.

This section describes how various supervised learning algorithms, such as RF, artificial neural networks, XGBoost, perform when faced with attack detection and classification in IoT environments. We will also highlight the specific contexts in which each algorithm excels and the trade-offs they impose in terms of computational complexity, accuracy, and robustness in the face of unbalanced data.

4.1. Analysis of Performance Indicators: Precision, Recall, Accuracy and F1-Score

The performance evaluation of the ten learning algorithms is primarily based on essential standard metrics: accuracy, precision, recall, and F1-score. These indicators provide a comprehensive and detailed perspective, enabling the assessment of both the models' ability to classify instances correctly and their capacity to handle the increasing complexity of intrusion detection in a modern IoT environment. Table 1 presents the main hyperparameters configured for each model. The analysis of the results obtained using the Macro Average as the performance metric aggregation method, as summarized in Table 2, highlights a clear hierarchy among the different approaches.

CNN demonstrates strong performance with an accuracy of 98.33% and a precision of 71.18%, showing its excellent capacity to capture complex patterns in network traffic data. This performance aligns well with other deep learning approaches, as evidenced by the strong results of LSTM (97.60% accuracy) and GRU (96.87% accuracy). The collective excellence of deep neural approaches can be explained by their intrinsic ability to learn sophisticated hierarchical representations of attack patterns, a crucial advantage in the dynamic and complex context of IoT security.

Among traditional algorithms, RF emerges as the top performer with the highest accuracy (99.29%) and precision (82.30%) among all studied algorithms. This performance is particularly significant in IoT, where managing false positives is a major challenge. XGBoost follows closely behind with impressive metrics (99.26% accuracy, 79.60% precision). In comparison, k-NN maintains solid performance with an accuracy of 94.66% and a precision of 68.26%, positioning itself as a viable alternative for resource-constrained systems.

Table 1. Models Configuration.

Model	Parameter Configuration	Values
XGBoost	Default parameters used	Default values
Naive Bayes (Gaussian)	Default parameters used	Default values
Random Forest	Default parameters used	Default values
Logistic Regression	random_state	42
LightGBM	Default parameters used	Default values
k-NN	n_neighbors (k)	k=5
Artificial Neural Network (ANN)	Input Layer	Input_dim=n_features
	Hidden Layers	[64, 32]
	Output Layer	Num_classes (34)
	Activation Functions	ReLU, Softmax
	Optimizer	Adam
	Loss Function	Categorical Crossentropy
	Batch Size	32
	Epochs	50
	Validation Split	0.2

Model	Parameter Configuration	Values
GRU (Gated Recurrent Unit)	Input Shape	(n_features, 1)
	GRU Layers	[128, 64]
	Dropout	0.3
	Dense Layers	[64,34]
	Activation Functions	ReLU, Softmax
	Optimizer	Adam
	Loss Function	Categorical Crossentropy
	Batch Size	32
	Epochs	50
	Validation Split	0.2
LSTM (Long Short-Term Memory)	Input Shape	(n_features, 1)
	LSTM Layers	[128, 64]
	Dropout	0.3
	Dense Layers	[64, 34]
	Activation Functions	ReLU, Softmax
	Optimizer	Adam
	Loss Function	Categorical Crossentropy
	Batch Size	32
	Epochs	50
	Validation Split	0.2
CNN (Convolutional Neural Network)	Input Shape	(n_features, 1)
	Conv1D Layers	[64, 32]
	Kernel Size	3
	Pool Size	2
	Dense Layers	[64, 34]
	Activation Layers	ReLU, Softmax
	Optimizer	Adam
	Loss Function	Categorical Crossentropy
	Batch Size	32
	Epochs	50
	Validation Split	0.2

Table 2. Comparative Analysis of Algorithm Performance Metrics.

Method	Accuracy	Precision	Recall	F1-Score
Naive Bayes (Gaussian)	0.5896	0.4387	0.3996	0.3069
Artificial Neural Networks (ANN)	0.9803	0.7006	0.6310	0.6469
Logistic Regression	0.8022	0.6218	0.4832	0.4887
k-Nearest Neighbors (k-NN)	0.9466	0.6826	0.6288	0.6395
XGBoost	0.9926	0.7960	0.7169	0.7291
Random Forest	0.9929	0.8230	0.7219	0.7355
LightGBM	0.3601	0.1206	0.1103	0.0824
GRU	0.9687	0.6166	0.6001	0.5926
LSTM	0.9760	0.6237	0.6179	0.6116
CNN	0.9833	0.7118	0.6472	0.6520

The comparison of recall metrics reveals interesting insights. RF and XGBoost lead with 72.19% and 71.69% recall rates, respectively, while deep learning algorithms maintain recall rates between 60-65%. While these levels are acceptable, they suggest room for improvement, which is particularly critical in IoT networks where an undetected attack could compromise the entire network.

The disappointing results of some algorithms deserve particular attention. The poor performance of LightGBM (36.01% accuracy, 12.06% precision) and NB (58.96% accuracy, 43.87% precision) contrasts sharply with their reputation in other application domains. This underperformance could be attributed to their difficulty handling the complexity and non-linearity inherent to attack patterns in IoT networks. Logistic Regression (LR), with an accuracy of 80.22%, demonstrates the limitations of linear approaches in this highly non-linear context.

The analysis of F1-scores shows that RF (0.7355) and XGBoost (0.7291) achieve the highest balanced performance, followed by CNN (0.6520) and ANN (0.6469). This hierarchy suggests that ensemble methods manage to maintain the best balance between detecting real attacks and minimizing false positives. The difference in F1-scores highlights the varying trade-offs made by each algorithm between precision and recall.

The general superiority of traditional ensemble approaches (RF, XGBoost) must be nuanced by practical considerations. While deep learning approaches show strong performance, their computational complexity and resource requirements can represent a significant obstacle in some IoT contexts, particularly for edge devices with limited computing capabilities. In such situations, lighter algorithms like k-NN can better compromise performance and resource efficiency.

This thorough analysis allows us to formulate precise contextual recommendations. RF or XGBoost architectures represent the optimal choice for critical IoT systems where maximum accuracy is paramount. RF offers the best trade-off in large-scale deployments where managing false positives is critical. For systems with significant resource constraints, k-NN presents a balanced alternative. Interestingly, more complex architectures like GRU and LSTM do not provide decisive advantages over CNN in this context, suggesting that algorithmic sophistication is not always synonymous with better performance.

4.2. Analysis and Evaluation Based on Confusion Matrices

Analyzing the diagonal values of confusion matrices reveals significant insights into the performance of different network intrusion detection algorithms. The main diagonal represents correct classifications for each traffic class, directly measuring each model's accuracy. XGBoost demonstrates remarkably high performance for most attack classes. Diagonal values close to 1 are observed for critical classes such as DDoS-SynonymousIP_Flood, DoS-SYN_Flood, and MITM-ArpSpoofing, indicating an almost perfect ability to identify these specific threats. Conversely, some models exhibit notable weaknesses for certain attack classes. The NB model shows significantly lower performance, with very low diagonal values for attacks such as SqlInjection, Uploading_Attack, and several DDoS variants.

The graphical visualization (Figure 3) reinforces these quantitative observations, allowing for an immediate visual interpretation of performance gaps between different algorithms. This graphical representation highlights accuracy variations particularly strikingly, complementing the numerical analysis. Deep learning algorithms, including ANN, CNNs, and models like LSTM and GRU, demonstrate remarkable robustness across different attack classes. This performance suggests their superior ability to capture complex patterns in network traffic data. This detailed analysis of confusion matrices highlights the importance of algorithm selection in network intrusion detection, emphasizing that performance can vary significantly depending on the specific type of threat being detected.

4.3. Performance analysis using AUC scores

The analysis of Area Under the Curve (AUC) values reveals exceptional performance for most machine learning algorithms in detecting different classes of network attacks. The models XGBoost, ANN, LSTM, CNN, and GRU stand out with consistently high AUC values, close to 1.00 for almost all attack categories, indicating remarkably precise classification capabilities. This performance suggests a very high ability to discriminate between malicious and legitimate traffic types.

In contrast, the Naive Bayes(NB) and LightGBM models exhibit significantly lower performance, with AUC values often around 0.50 for many attack classes, which is equivalent to random classification. This difference highlights the variability in performance depending on the algorithm used. Specific attacks such as SqlInjection, Uploading_Attack, and XSS show lower AUC values, suggesting particular challenges in their accurate detection. Conversely,

most models almost perfectly identify attacks like DDoS-SYN_Flood and DoS-TCP_Flood. The graphical visualization (Figure 4) associated with these data would provide a more intuitive way to highlight these variations in performance across different algorithms and attack types.

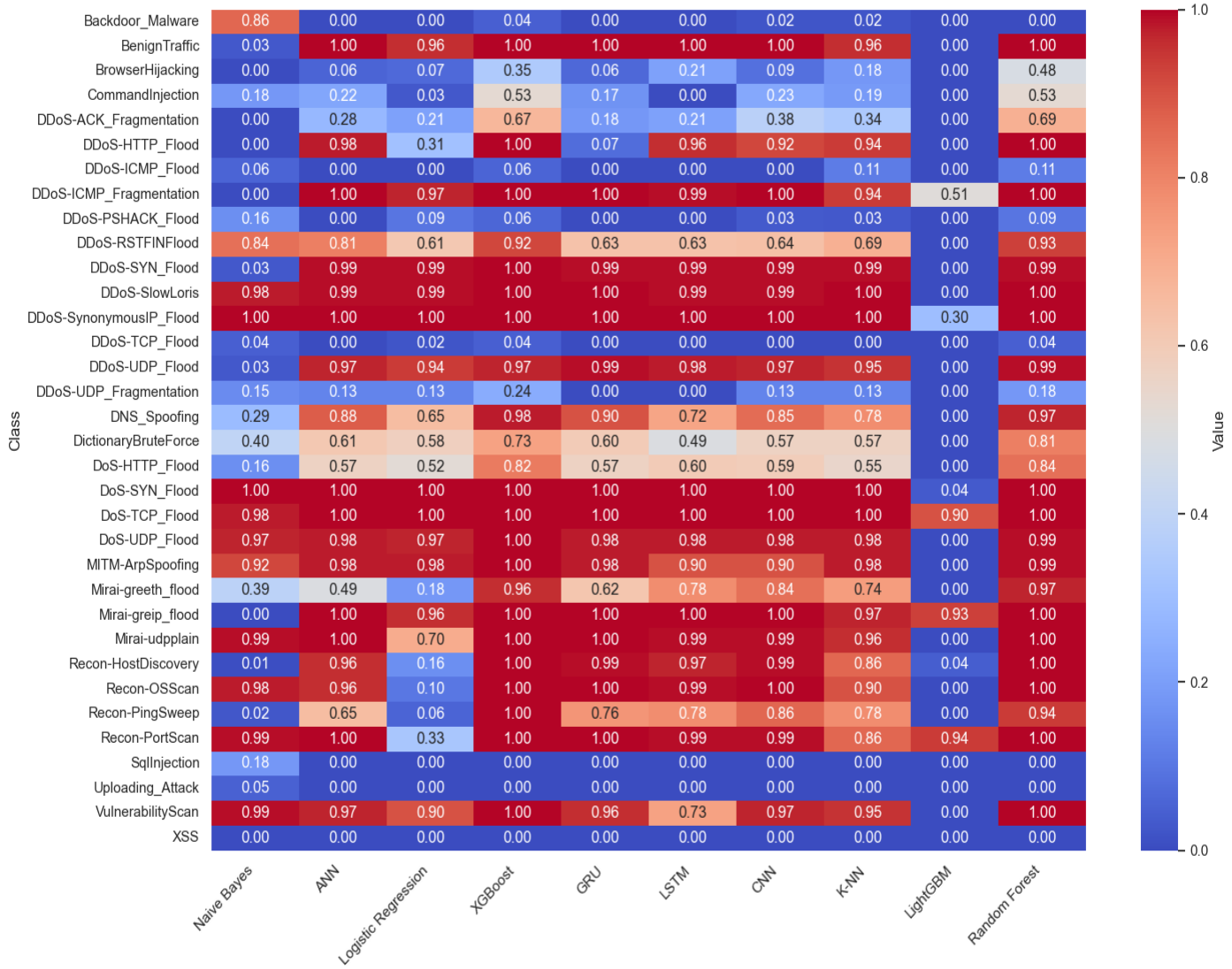

Figure 3. Confusion Matrix - Main Diagonal Values

5. Discussion of Results

The in-depth analysis of the ten learning algorithms evaluated in this study, using the Macro Average, reveals significant trends in IoT intrusion detection, particularly regarding the impact of class imbalance on model performance. The obtained results require a nuanced interpretation, considering the observed disparity between accuracy and other performance metrics.

The strong performance of deep learning approaches, notably CNN with 98.33% accuracy and 71.18% precision, must be interpreted in the context of significant imbalance between attack classes. This high accuracy and 64.72% recall reflect the models' tendency to perform better in most classes. This phenomenon is also observable for LSTM (97.60% accuracy) and GRU (96.87% accuracy), where the gaps between accuracy and other metrics suggest unbalanced performance across different attack classes.

Among traditional approaches, RF stands out with the highest overall precision (82.30%) and accuracy (99.29%), a particularly relevant result in the IoT context where managing false positives represents a major challenge. XGBoost follows closely with impressive performance

(99.26% accuracy, 79.60% precision), demonstrating a strong ability to handle class imbalance. The k-NN algorithm, with 94.66% accuracy, also maintains balanced performance, positioning itself as a viable alternative for resource-constrained systems.

The analysis of confusion matrices reveals varying success in classifying certain specific attacks. For instance, RF shows strong performance in detecting DDoS-HTTP_Flood (1.0), DNS_Spoofing (0.97), and Mirai-greeth_flood (0.97), while struggling with attacks like Backdoor_Malware (0.0) and SqlInjection (0.0). The ROC curves and AUC scores confirm these trends, with most algorithms achieving near-perfect AUC scores (1.0) for many attack classes, though performance varies significantly for certain attack types.

While balancing metrics such as recall and specificity is crucial in fields like clinical settings, where it enables more accurate and safer treatment decisions[63], and high accuracy plays a critical role in fraud detection by minimizing false alarms and ensuring genuine transactions are not mistakenly flagged as fraudulent [64], intrusion detection in IoT poses unique challenges that demand a different approach to metric prioritization.

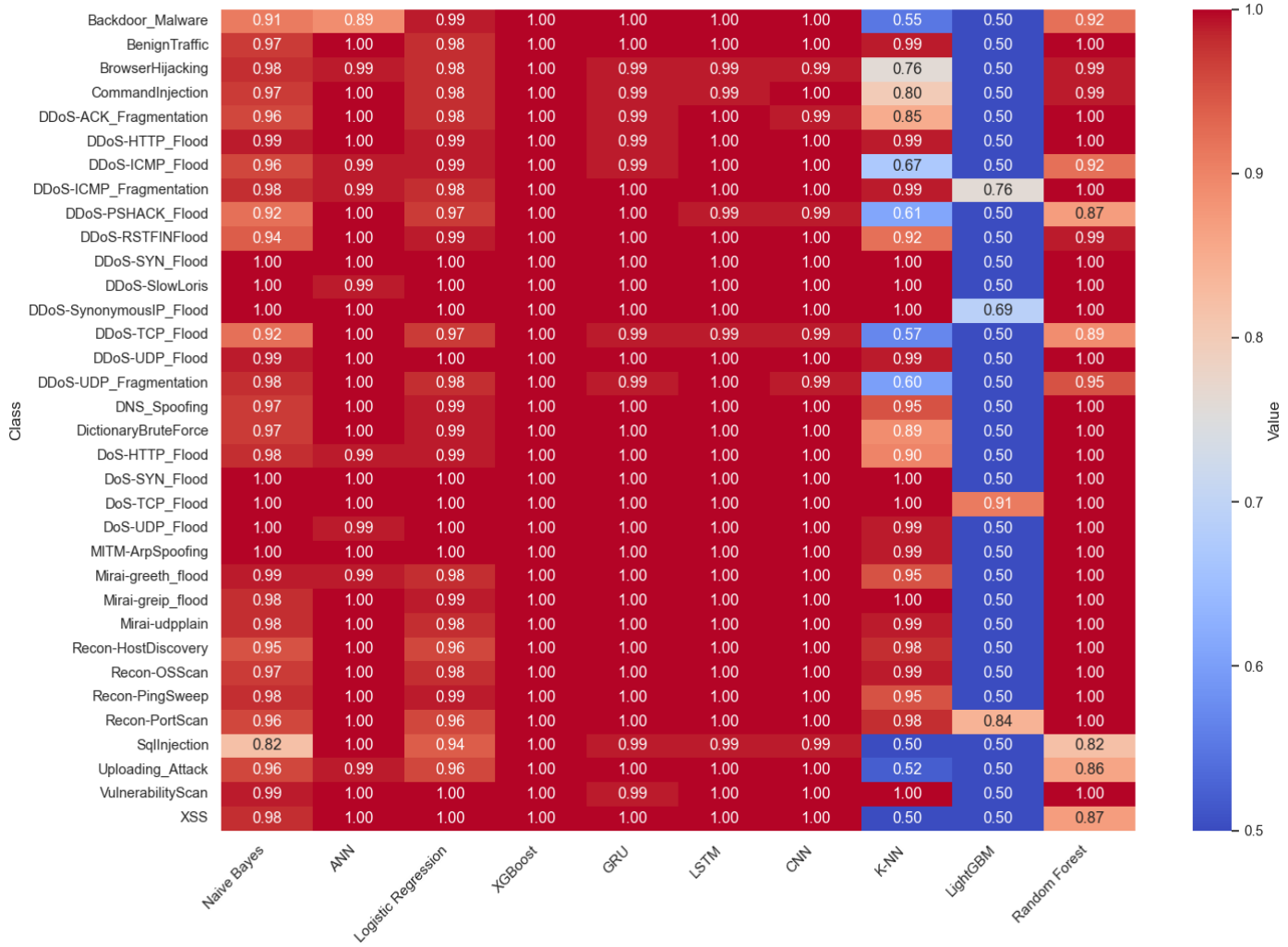

Figure 4. Receiver Operating Characteristic-AUC scores

The relatively strong F1-scores of the best algorithms (RF: 0.7355, XGBoost: 0.7291, CNN: 0.6520) take on added significance in the IoT context. These scores reflect a crucial trade-off between precision and recall, where false positives and negatives carry significant operational costs. The disappointing performance of certain algorithms, notably LightGBM (36.01% accuracy) and NB (58.96% accuracy), can be explained not only by their difficulty in handling the non-linearity of attack patterns but also by their sensitivity to class imbalance. LR, with 80.22% accuracy, demonstrates the limitations of linear approaches in this highly non-linear and imbalanced context.

Regarding practical recommendations, our analysis suggests that for critical IoT systems where precise attack detection is paramount, EF or XGBoost architectures represent the optimal choice despite class imbalance. This aligns with recent findings by Chirra[65], who demonstrated that ensemble approaches can better balance the preci-sion-recall trade-off in IoT security contexts. For large-scale deployments where managing false positives is critical, RF offers the best trade-off, which is particularly important in scenarios where security teams must efficiently allocate investigation resources. Systems with significant resource constraints will benefit from the k-NN approach, which maintains balanced performance despite imbalanced classes.

This analysis highlights a crucial distinction between traditional cybersecurity domains and IoT security: while high precision remains important, the potentially catastrophic impact of missed attacks in IoT environments necessitates equal attention to recall. As demonstrated by [66], the interconnected nature of IoT systems creates a unique security landscape where both false positives and false negatives must be carefully managed. Future research should focus on developing algorithms to optimize this crucial balance, particularly in edge computing and resource-constrained IoT devices.

6. Conclusion, Recommendations, and Future Perspectives

The comprehensive evaluation of ten supervised learning algorithms using the CICIoT2023 dataset has revealed significant insights into IoT network protection. Traditional ensemble approaches have demonstrated superior capabilities, with RF achieving 99.29% accuracy and 82.30% precision, followed closely by XGBoost (99.26% accuracy, 79.60% precision). Deep learning approaches have also shown strong performance, with CNN achieving 98.33% accuracy and 71.18% precision, followed by LSTM (97.60% accuracy) and GRU (96.87% accuracy). The observed disparity between accuracy metrics and other performance indicators across all algorithms highlights the significant impact of class imbalance in IoT attack detection.

These findings directly align with the research objectives by demonstrating that while ensemble learning approaches offer superior raw performance, their practical implementation requires careful consideration of multiple factors. The analysis of confusion matrices reveals varying success in detecting specific attack types, with some algorithms showing perfect detection rates for certain attacks (e.g., DoS-SYN_Flood, DDoS-SynonymousIP_Flood) while struggling with others (e.g., SqlInjection, XSS). This understanding has led to identifying optimal algorithms for specific deployment scenarios, with RF or XGBoost architectures proving most suitable for critical systems, RF for large-scale deployments requiring precise false positive management, and k-NN for resource-constrained environments.

The study makes several significant contributions to IoT security research and practice by establishing a comprehensive framework for evaluating intrusion detection systems in IoT environments. The analysis of AUC values demonstrates the robust discriminative ability of most algorithms across various attack types, with many achieving near-perfect scores (1.0) for numerous attack classes. This highlights the potential for highly effective detection systems when properly implemented. Furthermore, the research highlights the impact of class imbalance on detection performance and demonstrates the need for context-aware detection strategies in IoT environments.

Looking forward, several promising research directions warrant further investigation. The development of adaptive learning systems capable of dynamically adjusting precision-recall trade-offs based on context remains a crucial area for exploration. The particularly poor performance of LightGBM (36.01% accuracy) and the relatively modest performance of NB (58.96% accuracy) suggest opportunities for improving traditional algorithms' resilience to class imbalance. Research into lightweight deep learning architectures designed explicitly for resource-constrained IoT environments could significantly improve practical implementations. The investigation of hybrid approaches combining multiple algorithms to leverage their strengths shows promise for enhancing detection capabilities, particularly given the complementary strengths demonstrated in the confusion matrices. Additionally, the integration of explainable AI could help security teams better understand and validate detection decisions. In contrast, new techniques for handling class imbalance in IoT attack detection could improve overall system performance.

IoT networks' continuous evolution and security challenges necessitate ongoing research in these directions to develop more effective and efficient protection mechanisms. As IoT deployments continue to expand and diversify, the insights gained from this study provide a foundation for developing more robust and adaptable security solutions that can effectively protect increasingly complex IoT ecosystems while maintaining practical feasibility in real-world deployments. The demonstrated success of ensemble methods, particularly RF and XGBoost, suggests that future research should focus on enhancing these approaches while addressing their current limitations in detecting certain types of attacks.

Author Contributions: Conceptualization: Jean Pierre Ntayagabiri; methodology, Jean Pierre Ntayagabiri; software: Jean Pierre Ntayagabiri.; validation: Jean Pierre Ntayagabiri, Hind El Makhtoum, Youssef Bentaleb and Jeremie Ndikumagenge; formal analysis: Jean Pierre Ntayagabiri; investigation: Jean Pierre Ntayagabiri and Hind El Makhtoum.; writing original draft preparation: Jean Pierre Ntayagabiri.; writing review and editing: Jean Pierre Ntayagabiri.; supervision: Youssef Bentaleb and Jeremie Ndikumagenge. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The dataset used is a public dataset that was published by [38]. Direct access to its official repository is available at: https://www.unb.ca/cic/datasets/index.html

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8182–8201, Oct. 2019, doi: 10.1109/JIOT.2019.2935189.

[2] A. K. Goel, A. Rose, J. Gaur, and B. Bhushan, "Attacks, Countermeasures and Security Paradigms in IoT," in *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, Jul. 2019, vol. 1, pp. 875–880. doi: 10.1109/ICICICT46008.2019.8993338.

[3] J. P. Ntayagabiri, Y. Bentaleb, J. Ndikumagenge, and H. EL Makhtoum, "A Comprehensive Approach to Protocols and Security in Internet of Things Technology," *J. Comput. Theor. Appl.*, vol. 2, no. 3, pp. 324–341, Dec. 2024, doi: 10.62411/jcta.11660.

[4] I. Ahmad, M. Basheri, M. J. Iqbal, and A. Rahim, "Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection," *IEEE Access*, vol. 6, pp. 33789–33795, Jan. 2018, doi: 10.1109/ACCESS.2018.2841987.

[5] A. Çetin and S. Öztürk, "Comprehensive Exploration of Ensemble Machine Learning Techniques for IoT Cybersecurity Across Multi-Class and Binary Classification Tasks," *J. Futur. Artif. Intell. Technol.*, vol. 1, no. 4, pp. 371–384, Feb. 2025, doi: 10.62411/faith.3048-3719-51.

[6] J. A. B. Angelin and C. Priyadharsini, "Deep Learning based Network based Intrusion Detection System in Industrial Internet of Things," in *2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*, Jan. 2024, pp. 426–432. doi: 10.1109/IDCIoT59759.2024.10467510.

[7] P. K. Mall *et al.*, "A comprehensive review of deep neural networks for medical image processing: Recent developments and future opportunities," *Healthc. Anal.*, vol. 4, p. 100216, Dec. 2023, doi: 10.1016/j.health.2023.100216.

[8] L. Ding, W. Fang, H. Luo, P. E. D. Love, B. Zhong, and X. Ouyang, "A deep hybrid learning model to detect unsafe behavior: Integrating convolution neural networks and long short-term memory," *Autom. Constr.*, vol. 86, pp. 118–124, Jan. 2018, doi: 10.1016/j.autcon.2017.11.002.

[9] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System," *IEEE Access*, vol. 10, pp. 99837–99849, Jan. 2022, doi: 10.1109/ACCESS.2022.3206425.

[10] M. Fatima, O. Rehman, I. M. H. Rahman, A. Ajmal, and S. J. Park, "Towards Ensemble Feature Selection for Lightweight Intrusion Detection in Resource-Constrained IoT Devices," *Futur. Internet*, vol. 16, no. 10, p. 368, Oct. 2024, doi: 10.3390/fi16100368.

[11] Z. A. Al Waisi, "Optimized Monitoring and Detection of Internet of Things resources-constraints Cyber Attacks," *IMT School for Advanced Studies Lucca eprints*, Jan. 21, 2023. http://e-theses.imtlucca.it/392/

[12] S. Mishra, T. Anithakumari, R. Sahay, R. K. Shrivastava, S. N. Mohanty, and A. H. Shahid, "LIRAD: lightweight tree-based approaches on resource constrained IoT devices for attack detection," *Cluster Comput.*, vol. 28, no. 2, p. 140, Jan. 2024, doi: 10.1007/s10586-024-04792-x.

[13] M. Fatima, O. Rehman, S. Ali, and M. F. Niazi, "ELIDS: Ensemble Feature Selection for Lightweight IDS against DDoS Attacks in Resource-Constrained IoT Environment," *Futur. Gener. Comput. Syst.*, vol. 159, pp. 172–187, Oct. 2024, doi: 10.1016/j.future.2024.05.013.

[14] A. R. Khan, A. Yasin, S. M. Usman, S. Hussain, S. Khalid, and S. S. Ullah, "Exploring Lightweight Deep Learning Solution for Malware Detection in IoT Constraint Environment," *Electronics*, vol. 11, no. 24, p. 4147, Jan. 2022, doi: 10.3390/electronics11244147.
[15] Z. Alwaisi, T. Kumar, E. Harjula, and S. Soderi, "Securing constrained IoT systems: A lightweight machine learning approach for anomaly detection and prevention," *Internet of Things*, vol. 28, p. 101398, Jan. 2024, doi: 10.1016/j.iot.2024.101398.
[16] U. J. Otokwala, "Lightweight intrusion detection of attacks on the Internet of Things (IoT) in critical infrastructures.," Jan. 2024, doi: 10.48526/rgu-wt-2571244.
[17] T. Dias, N. Oliveira, N. Sousa, I. Praça, and O. Sousa, "A Hybrid Approach for an Interpretable and Explainable Intrusion Detection System," in *Intelligent Systems Design and Applications*, vol. 418, A. Abraham, N. Gandhi, T. Hanne, T.-P. Hong, T. Nogueira Rios, and W. Ding, Eds. Cham: Springer International Publishing, 2022, pp. 1035–1045. [Online]. Available: https://link.springer.com/10.1007/978-3-030-96308-8_96
[18] T. Zhong and J. Li, "Ransomware Detection with Machine Learning by Applying the Lapranove Function on Bytecode." May 30, 2024. doi: 10.31219/osf.io/zk3sw.
[19] I. Zakariyya, H. Kalutarage, and M. O. Al-Kadri, "Towards a robust, effective and resource efficient machine learning technique for IoT security monitoring," *Comput. Secur.*, vol. 133, p. 103388, Jan. 2023, doi: 10.1016/j.cose.2023.103388.
[20] H. Taherdoost, "Deep Learning and Neural Networks: Decision-Making Implications," *Symmetry (Basel).*, vol. 15, no. 9, p. 1723, Jan. 2023, doi: 10.3390/sym15091723.
[21] O. A. Alimi, K. Ouahada, and A. M. Abu-Mahfouz, "A Review of Machine Learning Approaches to Power System Security and Stability," *IEEE Access*, vol. 8, pp. 113512–113531, Jan. 2020, doi: 10.1109/ACCESS.2020.3003568.
[22] S. Muneer, U. Farooq, A. Athar, M. Ahsan Raza, T. M. Ghazal, and S. Sakib, "A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection: A Comprehensive Analysis," *J. Eng.*, vol. 2024, no. 1, p. 3909173, Jan. 2024, doi: 10.1155/2024/3909173.
[23] A. H. Abdi *et al.*, "Security Control and Data Planes of SDN: A Comprehensive Review of Traditional, AI, and MTD Approaches to Security Solutions," *IEEE Access*, vol. 12, pp. 69941–69980, Jan. 2024, doi: 10.1109/ACCESS.2024.3393548.
[24] Olakunle Abayomi Ajala, Chinwe Chinazo Okoye, Onyeka Chrisanctus Ofodile, Chuka Anthony Arinze, and Obinna Donald Daraojimba, "Review of AI and machine learning applications to predict and Thwart cyber-attacks in real-time," *Magna Sci. Adv. Res. Rev.*, vol. 10, no. 1, pp. 312–320, Feb. 2024, doi: 10.30574/msarr.2024.10.1.0037.
[25] S. O. Ooko and S. M. Karume, "Application of Tiny Machine Learning in Predicative Maintenance in Industries," *J. Comput. Theor. Appl.*, vol. 2, no. 1, pp. 131–150, Aug. 2024, doi: 10.62411/jcta.10929.
[26] A. Kumar, A. K. Singh, S. S. Ali, and B. J. Choi, "Expand and Shrink: Federated Learning with Unlabeled Data Using Clustering," *Sensors*, vol. 23, no. 23, p. 9404, Jan. 2023, doi: 10.3390/s23239404.
[27] S. P. Anh and Y. Nakamura, "A Baseline Investigation into the Evolution and Prevalence of Mirai and Hajime Utilizing a Network Telescope," *IEEE Access*, Jan. 2024, [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10613408/
[28] M. Kulbacki *et al.*, "A Review of the Weaponization of IoT: Security Threats and Countermeasures," Jan. 2024, pp. 279–284. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10619778/
[29] H. Jin, G. Jeon, H. W. A. Choi, S. Jeon, and J. T. Seo, "A threat modeling framework for IoT-Based botnet attacks," *Heliyon*, vol. 10, no. 20, Jan. 2024, [Online]. Available: https://www.cell.com/heliyon/fulltext/S2405-8440(24)15223-1
[30] H. Almazarqi, "Profiling IoT botnet activity," University of Glasgow, 2024. [Online]. Available: https://theses.gla.ac.uk/id/eprint/84102
[31] M. Gelgi, Y. Guan, S. Arunachala, M. Samba Siva Rao, and N. Dragoni, "Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques," *Sensors*, vol. 24, no. 11, p. 3571, Jun. 2024, doi: 10.3390/s24113571.
[32] E.-M. Călin, "IoT and Critical Infrastructures: Technological Transformation And Security Implications," in *Proceedings-The 20th International Scientific Conference "Strategies XXI" Technologies–Military Applications, Simulation And Resources*, Jan. 2024, pp. 386–394. [Online]. Available: https://www.ceeol.com/search/chapter-detail?id=1251750
[33] P. Kumari and A. K. Jain, "A comprehensive study of DDoS attacks over IoT network and their countermeasures," *Comput. Secur.*, vol. 127, p. 103096, Apr. 2023, doi: 10.1016/j.cose.2023.103096.
[34] K. B. Adedeji, A. M. Abu-Mahfouz, and A. M. Kurien, "DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges," *J. Sens. Actuator Networks*, vol. 12, no. 4, p. 51, Jul. 2023, doi: 10.3390/jsan12040051.
[35] A. Pakmehr, A. Aßmuth, N. Taheri, and A. Ghaffari, "DDoS attack detection techniques in IoT networks: a survey," *Cluster Comput.*, vol. 27, no. 10, pp. 14637–14668, Jan. 2024, doi: 10.1007/s10586-024-04662-6.
[36] R. Hallman, J. Bryan, G. Palavicini, J. Divita, and J. Romero-Mariona, "IoDDoS — The Internet of Distributed Denial of Sevice Attacks - A Case Study of the Mirai Malware and IoT-Based Botnets," in *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security*, Jan. 2017, pp. 47–58. doi: 10.5220/0006246600470058.
[37] N. Singh, R. Buyya, and H. Kim, "Securing Cloud-Based Internet of Things: Challenges and Mitigations," *Sensors*, vol. 25, no. 1, p. 79, Jan. 2025, doi: 10.3390/s25010079.
[38] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment," *Sensors*, vol. 23, no. 13, p. 5941, Jun. 2023, doi: 10.3390/s23135941.
[39] N. Koroniotis, N. Moustafa, E. Sitnikova, and J. Slay, "Towards Developing Network Forensic Mechanism for Botnet Activities in the IoT Based on Machine Learning Techniques," in *Mobile Networks and Management*, vol. 235, J. Hu, I. Khalil, Z. Tari, and S. Wen, Eds. Cham: Springer International Publishing, 2018, pp. 30–44. doi: 10.1007/978-3-319-90775-8_3.
[40] E. Hodo *et al.*, "Threat analysis of IoT networks using artificial neural network intrusion detection system," in *2016 International Symposium on Networks, Computers and Communications (ISNCC)*, May 2016, pp. 1–6. doi: 10.1109/ISNCC.2016.7746067.

[41] J. K. Samriya, R. Tiwari, X. Cheng, R. K. Singh, A. Shankar, and M. Kumar, "Network intrusion detection using ACO-DNN model with DVFS based energy optimization in cloud framework," *Sustain. Comput. Informatics Syst.*, vol. 35, p. 100746, Sep. 2022, doi: 10.1016/j.suscom.2022.100746.
[42] A. Deshmukh and K. Ravulakollu, "An Efficient CNN-Based Intrusion Detection System for IoT: Use Case Towards Cybersecurity," *Technologies*, vol. 12, no. 10, p. 203, Jan. 2024, doi: 10.3390/technologies12100203.
[43] A. Javad *et al.*, "Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced Anomaly Detection in High-Dimensional Datasets," *Eng. Technol. Appl. Sci. Res.*, vol. 14, no. 6, p. 17894, Jan. 2024, [Online]. Available: https://engagedscholarship.csuohio.edu/bus_facpub/356/
[44] R. A. Disha and S. Waheed, "A Comparative study of machine learning models for Network Intrusion Detection System using UNSW-NB 15 dataset," in *2021 International Conference on Electronics, Communications and Information Technology (ICECIT)*, Jan. 2021, pp. 1–5. doi: 10.1109/ICECIT54077.2021.9641471.
[45] A. Shehadeh, H. ALTaweel, and A. Qusef, "Analysis of Data Mining Techniques on KDD-Cup'99, NSL-KDD and UNSW-NB15 Datasets for Intrusion Detection," in *2023 24th International Arab Conference on Information Technology (ACIT)*, Jan. 2023, pp. 1–6. doi: 10.1109/ACIT58888.2023.10453884.
[46] F. Türk, "Analysis of Intrusion Detection Systems in UNSW-NB15 and NSL-KDD Datasets with Machine Learning Algorithms," *Bitlis Eren Üniversitesi Fen Bilim. Derg.*, vol. 12, no. 2, pp. 465–477, Jan. 2023, doi: 10.17798/bitlisfen.1240469.
[47] S. Choudhary and N. Kesswani, "Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 datasets using deep learning in IoT," *Procedia Comput. Sci.*, vol. 167, pp. 1561–1573, Jan. 2020, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050920308334
[48] G. Kocher and G. Kumar, "Analysis of Machine Learning Algorithms with Feature Selection for Intrusion Detection Using UNSW-NB15 Dataset." Social Science Research Network, Rochester, NY, Jan. 21, 2021. doi: 10.2139/ssrn.3784406.
[49] A. Dickson and C. Thomas, "Analysis of UNSW-NB15 Dataset Using Machine Learning Classifiers," 2021, pp. 198–207. doi: 10.1007/978-981-16-0419-5_16.
[50] S. Kumar and D. N. K. Pathak, "Evaluation Of Machine Learning Algorithms For Intrusion Detection Utilizing UNSW-NB15 Dataset," *J. Pharm. Negat. Results*, pp. 4819–4832, Jan. 2022, doi: 10.47750/pnr.2022.13.S08.630%20.
[51] K. Pramilarani and P. Vasanthi Kumari, "Cost based Random Forest Classifier for Intrusion Detection System in Internet of Things," *Appl. Soft Comput.*, vol. 151, p. 111125, Jan. 2024, doi: 10.1016/j.asoc.2023.111125.
[52] M. Ge, J. B. Hong, W. Guttmann, and D. S. Kim, "A framework for automating security analysis of the internet of things," *J. Netw. Comput. Appl.*, vol. 83, pp. 12–27, Apr. 2017, doi: 10.1016/j.jnca.2017.01.033.
[53] M. S. Mahdavinejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi, and A. P. Sheth, "Machine learning for internet of things data analysis: a survey," *Digit. Commun. Networks*, vol. 4, no. 3, pp. 161–175, Aug. 2018, doi: 10.1016/j.dcan.2017.10.002.
[54] M. Baich, T. Hamim, N. Sael, and Y. Chemlal, "Machine Learning for IoT based networks intrusion detection: a comparative study," *Procedia Comput. Sci.*, vol. 215, pp. 742–751, Jan. 2022, doi: 10.1016/j.procs.2022.12.076.
[55] S. V. N. Santhosh Kumar, M. Selvi, and A. Kannan, "A Comprehensive Survey on Machine Learning-Based Intrusion Detection Systems for Secure Communication in Internet of Things," *Comput. Intell. Neurosci.*, vol. 2023, no. 1, p. 8981988, Jan. 2023, doi: 10.1155/2023/8981988.
[56] A. Sajid, H. Abbas, and K. Saleem, "Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges," *IEEE Access*, vol. 4, pp. 1375–1384, Sep. 2016, doi: 10.1109/ACCESS.2016.2549047.
[57] G. Samara *et al.*, "A Comprehensive Review of Machine Learning-Based Intrusion Detection Techniques for IoT Networks," in *Artificial Intelligence, Internet of Things, and Society 5.0*, vol. 1113, A. Hannoon and A. Mahmood, Eds. Cham: Springer Nature Switzerland, 2023, pp. 465–473. doi: 10.1007/978-3-031-43300-9_38.
[58] B. Xu, L. Sun, X. Mao, R. Ding, and C. Liu, "IoT Intrusion Detection System Based on Machine Learning," *Electronics*, vol. 12, no. 20, p. 4289, Oct. 2023, doi: 10.3390/electronics12204289.
[59] C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," *IEEE Access*, vol. 5, pp. 21954–21961, Jan. 2017, doi: 10.1109/ACCESS.2017.2762418.
[60] I. Mbona and J. H. P. Eloff, "Detecting Zero-Day Intrusion Attacks Using Semi-Supervised Machine Learning Approaches," *IEEE Access*, vol. 10, pp. 69822–69838, Jan. 2022, doi: 10.1109/ACCESS.2022.3187116.
[61] J. M. Beaver, R. C. Borges-Hink, and M. A. Buckner, "An Evaluation of Machine Learning Methods to Detect Malicious SCADA Communications," in *2013 12th International Conference on Machine Learning and Applications*, Dec. 2013, vol. 2, pp. 54–59. doi: 10.1109/ICMLA.2013.105.
[62] C. S. Htwe, Z. T. T. Myint, and Y. M. Thant, "IoT Security Using Machine Learning Methods with Features Correlation," *J. Comput. Theor. Appl.*, vol. 2, no. 2, pp. 151–163, Aug. 2024, doi: 10.62411/jcta.11179.
[63] D. R. I. M. Setiadi, H. M. M. Islam, G. A. Trisnapradika, and W. Herowati, "Analyzing Preprocessing Impact on Machine Learning Classifiers for Cryotherapy and Immunotherapy Dataset," *J. Futur. Artif. Intell. Technol.*, vol. 1, no. 1, pp. 39–50, Jun. 2024, doi: 10.62411/faith.2024-2.
[64] M. I. Akazue, I. A. Debekeme, A. E. Edje, C. Asuai, and U. J. Osame, "UNMASKING FRAUDSTERS: Ensemble Features Selection to Enhance Random Forest Fraud Detection," *J. Comput. Theor. Appl.*, vol. 1, no. 2, pp. 201–211, Dec. 2023, doi: 10.33633/jcta.v1i2.9462.
[65] D. R. Chirra, "Deep Learning Techniques for Anomaly Detection in IoT Devices: Enhancing Security and Privacy," *Rev. Intel. Artif. en Med.*, vol. 14, no. 1, pp. 529–552, Jan. 2023, [Online]. Available: http://redcrevistas.com/index.php/Revista/article/view/214
[66] A. Jaramillo-Alcazar, J. Govea, and W. Villegas-Ch, "Anomaly Detection in a Smart Industrial Machinery Plant Using IoT and Machine Learning," *Sensors*, vol. 23, no. 19, p. 8286, Oct. 2023, doi: 10.3390/s23198286.